NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MOBILITY FOR GCSS-MC THROUGH VIRTUAL PCs

by

Steven K. Thompson

June 2017

Thesis Advisor: Arijit Das
Co-Advisor: Gurminder Singh

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE MOBILITY FOR GCSS-MC THROUGH VIRTUAL PCs			**5. FUNDING NUMBERS**
6. AUTHOR(S) Steven K. Thompson			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The ability for Marines to access Global Combat Support System-Marine Corps (GCSS-MC) through mobile devices such as tablets and smart phones would greatly improve their productivity. Mobile device access to GCSS-MC would allow Marines to access a required program for their mission using a form of computing device with which they are most familiar. Currently, there is not an approved mobile application designed for use with GCSS-MC or any approved mobile access method. Our research shows that the use of virtual PCs (VPCs) to access applications such as GCSS-MC is a secure and technologically feasible method to provide mobile access to GCSS-MC. By using VPCs, thin clients, such as mobile devices, are able to access computationally strenuous and high-network throughput applications with a device running on various operating systems with limited computational ability. The use of VPCs leads to a reduced need for network throughput and faster overall execution.

14. SUBJECT TERMS GCSS-MC, enterprise resource planning, virtual personal computer			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

MOBILITY FOR GCSS-MC THROUGH VIRTUAL PCs

Steven K. Thompson
Major, United States Marine Corps
B.S., Georgia Institute of Technology, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2017

Approved by: Arijit Das
Thesis Advisor

Gurminder Singh
Co-Advisor

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The ability for Marines to access Global Combat Support System-Marine Corps (GCSS-MC) through mobile devices such as tablets and smart phones would greatly improve their productivity. Mobile device access to GCSS-MC would allow Marines to access a required program for their mission using a form of computing device with which they are most familiar. Currently, there is not an approved mobile application designed for use with GCSS-MC or any approved mobile access method. Our research shows that the use of virtual PCs (VPCs) to access applications such as GCSS-MC is a secure and technologically feasible method to provide mobile access to GCSS-MC. By using VPCs, thin clients, such as mobile devices, are able to access computationally strenuous and high-network throughput applications with a device running on various operating systems with limited computational ability. The use of VPCs leads to a reduced need for network throughput and faster overall execution.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ATLASS	Asset Tracking Logistics and Supply System
DOD	Department of Defense
ERP	Enterprise Resource Planning
GCSS-MC	Global Combat Support System-Marine Corps
GPDLs	Government Provided Desktops and Laptops
GPU	Graphics Processing Unit
IaaS	Infrastructure as a Service
ISDN	Integrated services digital network
HDX	High Definition User Experience
HTML	Hypertext Markup Language
IT	Information Technology
LAN	Local area network
MAGTF	Marine Air Ground Task Force
MCEN	Marine Corps Enterprise Network
MFS	Mobile Field Services
MIMMS	Marine Corps Integrated Maintenance System
NIST	National Institute of Standards and Technology
OS	Operating System
OSI	Open systems interconnection
PaaS	Platform as a Service
PC	Personal Computer
PC-MIMS	Personal Computer- Marine Corps Integrated Maintenance System
PCoIP	Personal Computer over Internet Protocol
POTS	Plain old telephone services
RADIUS	Remote Authentication Dial-In User Service
RDP	Remote Desktop Protocol
RFB	Remote Framebuffer
RIP	Repairable Issue Point
SaaS	Software as a Service
SMU	Supply Management Unit

SQL	Structured Query Language
TAV	Total Asset Visibility
TCP	Transmission Control Protocol
TWMS	Tactical Warehouse Management System
UDP	User Datagram Protocol
UI	User Interface
VPC	Virtual Personal Computer
VPN	Virtual Private Network
WWW	World Wide Web

ACKNOWLEDGMENTS

First, I must thank my Creator for giving me the abilities to complete this program. Through Him, all things are possible. On my own, I could not have done any of this. Second, I would like to thank the Marine Corps for giving me this oppurtunity. I would also like to thank my family for the support that they have provided throughout my Marine Corps career and especially the last two years here at NPS. Finally, I would like to thank my advisors for keeping me on track and giving me the rudder steers as needed to complete this task.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

Global Combat Support System-Marine Corps (GCSS-MC) provides a deployable, single point of entry for all logistics requirements in the Marine Air-Ground Task Force (MAGTF). The goal of GCSS-MC is to speed up, streamline, and optimize the logistics process through reduction of antiquated paperwork previously associated with the ordering of supplies, executing logistics, and repairing equipment (United States Marine Corps [USMC] Concepts and Programs, 2015). GCSS-MC leverages the functionality of Oracle's E-Business Suite to manage the underlying database that provides the enterprise-wide access to Marine Corps assets. In the current implementation, GCSS-MC must be accessed by the supply, logistics, and maintenance Marines through a desktop or laptop workstation. Nearly all interaction with GCSS-MC occurs with the using Marines sitting in their workspaces. GCSS-MC operates on the Marine Corps Enterprise Network (MCEN), making the ability to access GCSS-MC from home or remote locations limited as users must have a Common Access Card (CAC) reader and a PC to access the MCEN. Moreover, there is no viable way to access GCSS-MC from a mobile device such as a tablet or smartphone.

B. PURPOSE

The purpose of this research is to provide Marine personnel with a technologically effective method to interact with GCSS-MC in mobile settings. This research evaluates the current model of accessing GCSS-MC through government-provided desktops and laptops (GPDLs) and explores the ability to use virtual PCs, to mobilize access to GCSS-MC. This research includes provisions to ensure for mobile access.

Finding an efficient manner for Marines to access and interact with GCSS-MC through the use of mobile devices will allow Marines more easily to complete their tasks and achieve mission accomplishment. Marines commonly access the World Wide Web (WWW) with mobile devices and are most comfortable using these devices. The ability to access GCSS-MC using the tools they are already familiar with has the potential to

raise the Marine's comfort level and productivity when interacting with GCSS-MC. Figure 1 illustrates the proposed architecture.

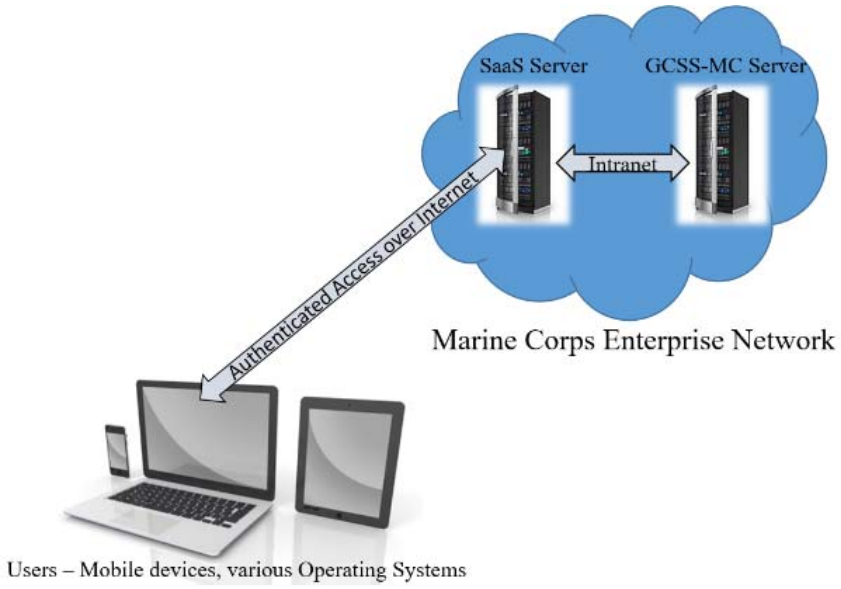

Figure 1. Proposed Software as a Service Architecture

C. PROBLEM STATEMENT

Supply, logistics, and maintenance Marines have minimal access to GCSS-MC outside of the MCEN workstations in their respective shops. There is currently no mobile solution for accessing GCSS-MC. A more flexible, versatile and most importantly, mobile solution is needed to support the supply, logistics and maintenance Marines who interact with GCSS-MC on a daily basis to achieve mission success. The ability of Marines to directly interact with GCSS-MC, through the use of a tablet or other mobile device would greatly improve the chance of Marines to achieve mission success. Additionally, the addition of mobile access to GCSS-MC would allow for Marines to interact with GCSS-MC with the type of device that is most commonly used by today's users and is the future of computing.

D. RESEARCH QUESTION

The primary research question is as follows:

- Is using the Software as a Service (SaaS) model, specifically virtual personal computers (VPCs), a technologically efficient alternative for mobile access to GCSS-MC?

E. SCOPE

This research specifically focuses on the use of VPCs to allow mobile access to GCSS-MC. VPCs are evaluated as a means to link GCSS-MC users to the GCSS-MC database independent of location or type of device. This research does not provide direct access to GCSS-MC from a mobile device, instead, it uses a VPC to provide this access.

There are multiple ways to access a large and complex system such as GCSS-MC from a mobile device such as purpose built mobile applications and mobile web access. This research focuses on using a VPC to provide the mobile access. There are advantages and disadvantages to each of these methods. The advantages to a purpose built mobile application include having an application that is specific to the work that needs to be done; however, when building a mobile application, there can drawbacks. The drawbacks include having to build the mobile application to function on a variety of devices and operating systems or risk being tied to a single device and single operating system. Mobile web access has a similar risk in that the mobile webpage may not display properly on the full range of mobile devices in use.

The use of VPCs combined with commercially available software allows for mobile access to a complex system such as GCSS-MC without having to change anything in the GCSS-MC architecture or how it is accessed. From the point of view of GCSS-MC, the VPC accessing GCSS-MC is the same as any PC accessing GCSS-MC. VPCs have the potential to ease security management as well because there is only one VPC image that must be maintained, allowing for security patches and updates to be applied quickly and easily. The possible disadvantage to using a VPC to access GCSS-MC include network connectivity and latency. This research evaluates VPC access using the high speed, high bandwidth network that is available on the Naval Postgraduate School Campus as well as access through the more constrained AT&T residential Internet.

F. RELEVANCE TO DOD

By developing a mobile access solution for GCSS-MC, the ability of supply, logistics, and maintenance Marines to conduct their mission essential tasks in more and varying locations, this will continue to further the Marine ethos of “any clime and place.” Additionally, the addition of mobile access to one Marine Corps system may open the doors for mobile access to other Marine Corps systems such as Marine Online, MarineNet, and the Marines College of Distance Education and Training. Furthermore, it follows the guidance given by Teresa Takai, which encourages the integration of mobile devices into the DOD information structure (Department of Defense Chief Information Officer, 2012, i).

G. THESIS OVERVIEW

1. Chapter I: Introduction

This chapter frames the problem that the thesis explores, introducing current hurdles to overcome so that mobile devices may interact with GCSS-MC and the MCEN.

2. Chapter II: Background

This chapter begins by describing the history and the architecture of GCSS-MC. It then proceeds to explore various architectures of cloud computing and methods of cloud computing can be employed to add mobile access to GCSS-MC. This chapter also describes the remote desktop protocols used to access VPCs. Additionally, this chapter explores possible security solutions when employing mobile access to the MCEN such as virtual private networks (VPN).

3. Chapter III: Experimental Design

This chapter outlines the design of the experiment in this thesis. It begins by exploring the contents of the copy of the GCSS-MC database that is being used to and developing queries with which to test the performance of accessing GCSS-MC with a mobile device through the use of a Software as a Service desktop.

4. Chapter IV: Testing and Results

Executing the designed experiment detailed in Chapter III, this chapter details the experiment as conducted along with the results of the experimentation.

5. Chapter V: Conclusions and Future Work

This chapter summarizes the research conducted in this thesis and details the conclusions drawn from the results of Chapter IV as well as explores areas of future research as related to this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter provides a survey of the technologies and systems that are investigated in the follow on chapters, beginning with a brief history of the Marine Corps' chosen solution to provide automated logistics support, GCSS-MC, along with the enabling technologies such as Oracle's E-Business Suite. It also discusses the benefits of Virtual PCs and Cloud computing as a solution to organizational needs to provide computing resources. Finally, this chapter reviews technological solutions to secure remote access utilizing remote desktop protocols and virtual private networks.

A. GLOBAL COMBAT SUPPORT SYSTEM-MARINE CORPS

In analysis of the implementation challeges related to Enterprise Resource Planning (ERP) Information Technology (IT) Systems, Mark Jones (2010) notes that more than three decades ago, the Department of Defense (DOD) set the goal of what it refers to as total asset visibility (TAV), a process by which all items owned by the DOD could be tracked and accounted for using automated systems. An ERP is a broad term used to refer to systems and software packages that organizations use to manage activities such as accounting and procurement with the goal of eliminating duplicate data and providing data integrity across multiple sources (Oracle 2016). Furthermore, Jones (2010) observes that the four services are implementing their own, service specific software with the Marine Corps and the Air Force opted for Oracle as their software provider, while the Army and the Navy opted for SAP SE.

Continuing his ERP analysis, Jones states that the Marine Corps' software solution called GCSS-MC, is a commercial off the shelf (COTS) Oracle solution (2010). He also asserts that GCSS-MC is built on Oracle's 11i E-Business Suite and is currently in release 1.1 and is designed to provide the sought after TAV and affords core logistics and business functionality (Jones 2010). GCSS-MC replaced several legacy systems such as Supported Activity Supply System (SASSY), Asset Tracking Logistics and Supply System (ATLASS), Marine Corps Integrated Maintenance Management System (MIMMS), and Personal Computer-MIMMS (PC-MIMMS) (Miller 2016). SASSY is a

prime example of the benefit of implementing an ERP, to eliminate legacy systems. SASSY was developed and implemented on mainframe computers from the 1970s and is programmed using the COBOL, which has been in use since 1959 (Jones 2010). Implementing a more modern approach than the 1950s and 1970s is needed.

USMC Programs and Concepts (2015) defines many of the future and current capabilities of GCSS-MC, using GCSS-MC, a supported unit can request anything from ordering repair parts or ordering maintenance for a particular end item. When the service request is complete, the supported unit can track the status of the service request by using an Internet-based Interface. The status of the service request includes things such as an inventory of repair parts and status of maintenance requests (USMC Concepts and Programs 2015). Furthermore, supporting units and higher units can also track the service request which provides readiness and logistics situational awareness across the MAGTF (USMC Concepts and Programs 2015). GCSS-MC Release 1.1 achieved the Full Deployment Decision acquisition milestone in March of 2015 (USMC Concepts and Programs 2015). Increment 1.1 offers the ability of users to access what was once managed by SASSY, MIMMS, PC-MIMMS, and ATLASS, in one single point of entry, making the use of these legacy systems redundant (USMC Concepts and Programs 2015). GCSS-MC release 1.2 will provide the same functionality to Marines deployed in austere environments with limited network connectivity to GCSS-MC services (Program Executive Office for Enterprise Information Systems [PEOEIS] 2017).

The goal of achieving a “deployable, single point of entry for all logistics requirements” is reachable by GCSS-MC and is well underway with the release 1.1 but will not be fully implemented until release 1.2 (PEOEIS 2017). Future increments of GCSS-MC will introduce even more capabilities. USMC Concepts and Programs plans for future increments to include two high-level modules. The first module is the Tactical Warehouse Management System (TWMS), and the second will be the Full Deployable Capability (2015). The TWMS will support the integration of two of the integrated retail-level warehouses within the current supply system, the Supply Management Unit (SMU), and the Repairable Issue Point (RIP) (USMC Concepts and Programs 2015). The SMU and the RIP are integral parts of the current logistics and supply infrastructure, and their

integration into the GCSS-MC architecture will greatly improve the functionality of GCSS-MC (USMC Concepts and Programs 2015). The second module, the Full Deployable Capability, will ensure that GCSS-MC is completely implemented even in austere environments with little to no network connectivity or access (USMC Concepts and Programs 2015). The Full Deployable Capability will ensure GCSS-MC access to all MAGTF units. Figure 2 depicts a high-level Operational concept for GCSS-MC. As shown in Figure 2, the fully implemented version of GCSS-MC, with both the TWMS and Full Deployable Capability modules completed, allowing the MAGTF Commander, and other affected personnel all the way to the Combatant Commander to have better situational awareness as to the logistics needs of supporting and supported units.

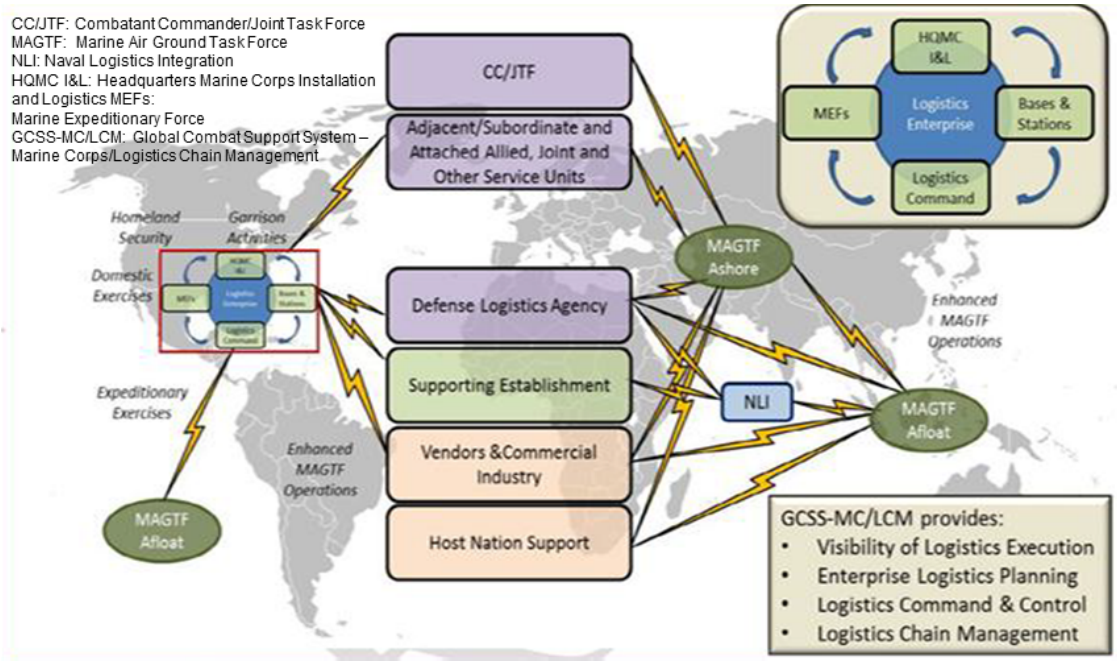

Figure 2. GCSS-MC High-Level Operational Concept.
Source: USMC Concepts and Programs (2015).

Figure 2 represents the end state of a fully developed GCSS-MC, not what is in current operation. A glaring example of features not yet implemented is the mobility that depicted in Figure 2. The amount of mobility currently built into GCSS-MC is implemented using two modes of operation, connected and disconnected mode (USMC

Concepts and Programs 2015). These two modes of operation are used regardless of the operational environment, whether in garrison, the field, or deployed (USMC Concepts and Programs 2015). In his thesis, Paxton Miller analyzes these operating modes, in disconnected mode, Mobile Field Services (MFS) caches changes and requests made by the user on the physical device operating GCSS-MC, sending these requests to the GCSS-MC servers upon the restoration of the network connectivity (2016). In the same analysis, when operating in connected mode, requests are sent over the Internet as they are made (2016). He also observes that in the full commercially available version, MFS allows for the use of mobile devices to access the E-Business Suite; however, GCSS-MC only authorizes GPDLs to utilize MFS, not mobile devices such as tablets or smartphones (2016).

B. ORACLE E-BUSINESS SUITE

GCSS-MC is built using the Oracle E-Business Suite. E-Business Suite provides a framework that allows for a distributed and multi-tiered system, built on a three-tier architecture (Farrington 2010). The three tiers are the desktop tier, the application tier, and the database tier (Farrington 2010). Each of the tiers is a logical grouping of services, each of these services can run on a single server, or depending on the throughput required, multiple servers (Farrington 2010). Figure 3 depicts this three-tiered architecture.

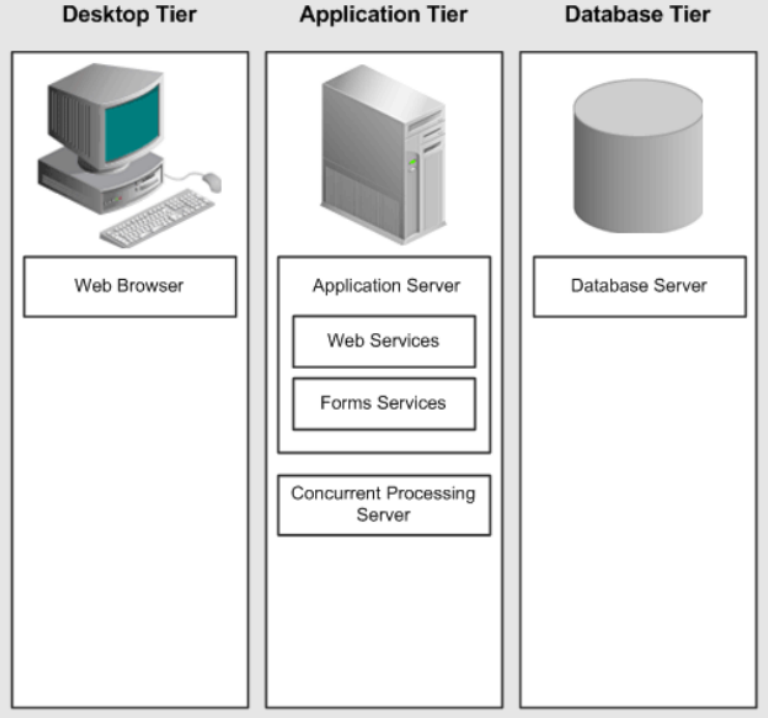

Figure 3. Oracle E-Business Suite Three Tier Architecture.
Source: Farrington (2010).

Robert Farrington, in the Oracle E-Business Suite Concepts, defines the first tier as the database tier, which manages the Oracle database (2010). The middle tier is referred to by Oracle as the application tier and manages the various components of the E-Business Suite. The third tier, Oracle calls the desktop tier (2010). The desktop tier provides the user interface (UI) to the E-Business Suite and is implemented through web browser add-ons (Farrington 2010). The three level architecture allows for application tier and the desktop tier to successfully communicate over a wide area network with varying levels of connectivity (Farrington 2010). Successful communication with varying connectivity is made possible because the two tiers minimize the amount of information exchanged between them (Farrington 2010). The minimization of communications between the Desktop and Application tiers frees resources for communications between the desktop and the database tier, and also reduces the costs associated with telecommunications, and it improves response times (Farrington 2010).

Examining the architecture components starting from the client through to the database starts with the desktop tier. Clients access the E-Business Suite through the desktop tier (Farrington 2010). From the desktop tier there are two methods of access, web based applications and desktop Java clients (Farrington 2010). Web based applications run a Java applet in a web browser, and the desktop Java clients are for forms-based products (Farrington 2010). To support forms-based products, Oracle E-Business Suite uses the Forms client applet, a general-purpose applet (Farrington 2010). The Desktop Java Clients are accessed through the Sun JRE Plug-in installed in a browser (Farrington 2010). The Desktop Java Clients allow for forms to run in a Java Virtual Machine (JVM) that is separate from the browser's JVM (Farrington 2010).

The next tier in the architecture moving from the client to the databases is the application tier. Oracle defines the application tier as having two roles—"hosting the various servers and service groups that process the business logic, and managing communication between the desktop tier and the database tier" (Farrington 2010). The application tier is further delineated into three service groups: web services, forms services, and concurrent processing services (Farrington 2010). The web services service group is responsible for processing requests from clients received over the network (Farrington 2010). The forms services service group provides the ability to employ network security fundamentals such as firewalls and proxy servers (Farrington 2010). Many tasks such as reporting programs, data updating programs, and other services that are computationally intensive, could disrupt user actions, the concurrent processing services service group allows for these tasks to be run in the background, freeing resources, allowing users to continue their work uninterrupted (Farrington 2010). If any of these three service groups are hosted on more than one physical machine, E-Business Suite supports load balancing between these services to provide for more consistent availability, reliability, scalability and fault tolerance (Farrington 2010).

The database tier is the final tier. The Oracle database server or servers reside in the database tier, the database server houses all of the information that is stored and administered by the E-Business Suite (Farrington 2010). Oracle has designed the database tier so that the "database server communicates with the services and servers on

the application tier" (Farrington 2010). The application tier then in turn communicates with the clients. Oracle makes the essential distinction that "there is no direct communication between the database and the clients" (Farrington 2010).

C. VIRTUAL PCs

1. VPCs: Defined

When discussing VPCs, a common language must first be established. There are several definitions of VPCs in common usage; to reduce confusion, we must first establish a set of definitions. A VPC, generically defined, is a PC running in a virtual environment, generally running on a more powerful machine which is hosting multiple operating systems (OS), with each OS running independent applications (*PC Magazine* 2017). Virtualization of PCs is a technique that makes it possible for the abstraction of various machines, processes, and applications, on one single machine (Barreto 2011). The software used to create and manage the logical instances of machines is known as a hypervisor (Barreto 2011).

The next standardized definition is that of a thin client, *PC Magazine* defines a thin client as "a machine that relies on a server to perform data processing" (2017). A thin client may be an underpowered machine, not capable of performing the computations, or a standard PC which is acting as a thin client. Further narrowing the definition thin clients, "a thin client does not process any data; it processes only the user interface" (*PC Magazine* 2017).

The third and final standard definition is desktop virtualization. Desktop virtualization is a "thin client architecture in which each user's desktop, which includes the operating system and applications, runs in a separated 'virtual machine' partition in a server on the network" (*PC Magazine* 2017). This architecture allows for each client's desktop to be delivered over the network, with all computing taking place at the server and the thin clients displaying only the (UI) (*PC Magazine* 2017). This architecture is also referred to client virtualization (*PC Magazine* 2017).

2. VPCs: History and Benefits

Examining the history of VPCs leads to the original IBM System 370 Mainframe computer from the early 1970s (Barreto 2011). The first documented instance of a VPC was the IBM System 370, paired with VM/370, the first virtual machine OS (Barreto 2011). This model continued to evolve through the 1970s and with the release of the IBM 5150 PC in 1981, it became possible to use relatively inexpensive devices to access much more capable servers to conduct the complex computations (Barreto 2011). This use of commodity devices to access the powerful and expensive servers is the root of the thin client and virtual desktop infrastructure that is in use today.

There are several benefits of using the underutilized physical resources of a powerful server to create VMs which are then accessed by far less powerful thin clients. The first and most applicable benefit is that the thin clients accessing the VM server can be running most any OS. The thin client could be running anything from Microsoft Windows or a Linux OS to a mobile OS such as Android or Apple's iOS (Barreto 2011). By making the virtual desktop infrastructure OS agnostic by accessing the VPCs through a web browser, we can greatly reduce the amount of software that must be managed by system administrators. Additionally, the devices that are connecting to the virtual desktop architecture do not have just varied OSs installed, they can represent vastly different hardware setups. Desktops, laptops, and mobile devices such as tablets or smartphones can serve as thin clients to access the virtual desktop infrastructure (Barreto 2011). Additionally, the use of an OS/Device agnostic architecture allows for system administrators to manage only one variety of applications for their particular needs. All of the mission critical software applications will be for the OS of the VPC that the system administrators choose to use. If the organization is using Windows, for instance, the organization is only required to maintain Windows compatible software; the system administrators do not have the need to support identical applications for Linux, Unix or any other OSs (Barreto 2011).

D. CLOUD COMPUTING

The use of VPCs has, in practice, evolved into what is referred to as cloud computing or the cloud. Cloud computing refers not just to applications delivered over the WWW, but also the hardware and systems that reside in data centers. (Armbrust et al. 2010, 50) The architecture of cloud computing consists of a broad spectrum of services and is classified into three large segments. Cloud computing is delineated into three main categories, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Figure 4 depicts these categories in what Ben Kepes (2017) calls the cloud computing stack; the top of the cloud computing stack is SaaS, which is "designed for end-users, and delivered over the web." PaaS is the second tier in the cloud computing stack, designed primarily for developers, giving them access to tools and services to enable quick and efficient application development. (Kepes 2017) Finally, IaaS is the broadest category of the cloud stack, comprised of the hardware that powers the cloud, the servers, storage, networks, and OSs that enable cloud computing. (Kepes 2017)

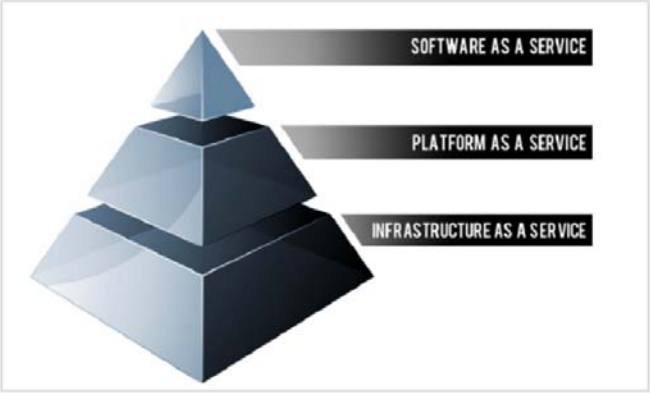

Figure 4. The Cloud Computing Stack. Source: Kepes (2017).

Cloud computing as defined by the National Institute of Standards (NIST) consists of several characteristics: "On-demand self-service," "Broad network access," "Resource pooling," "Rapid elasticity," and "Measured Service" (Grance and Mell 2011). The on-demand services characteristic seeks to minimize the user interaction and delays

that are associated with traditional IT services (Kepes 2017). The broad network access characteristic seeks to make the services widely available to users. The resource pooling characteristic seeks to eliminate the need for each user to have vast amounts of dedicated resources (Kepes 2017). Finally, the elasticity characteristic seeks to scale services as they are needed, expanding when necessary, and narrowing when not needed, scaling services provided with the demand for the services (Kepes 2017). This ability to scale services offers the appearance of infinite computing resources, reducing the amount of resource planning that is necessary to provision hardware (Armbrust, et al. 2010, 51).

IaaS is the base of the cloud computing stack depicted in Figure 4. When defining IaaS, NIST states that IaaS is providing the consumer with the ability to

> Provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components. (Grance and Mell 2011)

IaaS delivers the infrastructure that forms the Cloud Computing infrastructure—the servers, the storage, the routers, the switches, and any other required infrastructure to build a cloud. Instead of an organization spending the time and money to build a data center, IaaS offers the ability of an organization to immediately have access to a fully functional cloud, on demand (Kepes 2017). The often attributed characteristics of IaaS include distributed resources and services that have a utility-based pricing model (Kepes 2017). The situations where IaaS is the most sensible option is often for new organizations that may not possess the capital to procure the requisite hardware for their operation, or their organization is growing too rapidly and s outpacing hardware procurement to keep up (Kepes 2017). However, IaaS is not usually the best option for organizations that have the ability to procure the requisite hardware, or the security implications of outsourcing data storage and processing make it infeasible (Kepes 2017).

NIST defines PaaS as providing the consumer with the ability to “deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider” (Grance

and Mell 2011). PaaS brings many of the benefits of SaaS to software developers. PaaS does not deliver software to the developers. Instead, PaaS provides a platform used to create software (Kepes 2017). The characteristics that define PaaS are services to help develop and test applications in one integrated environment. PaaS must have a web-based UI, and multiple users must be able to access the same application. Finally, like IaaS, it needs to include billing management but is billed in a subscription style instead of a utility style (Kepes 2017). PaaS is the best fit for instances when multiple developers will be working on a single project or when developers want to automate testing of their services being developed (Kepes 2017). It is not the best solution if the developers are worried about provider lock-in or where the application development would require the underlying hardware to be customized to fit the developer's needs (Kepes 2017).

NIST defines SaaS as providing the consumer with "the ability to use the provider's applications running on a cloud infrastructure" (Grance and Mell 2011). SaaS is the best-known form of cloud computing, being the form of cloud computing that is most used by average users. Kepes lists the defining characteristics of SaaS as "web access to commercial software," software that "is managed from a central location," software that is "delivered in a 'one to many' model," and software that does not require the user to "handle software upgrades and patches" (Kepes 2017). SaaS makes the most sense for situations where many users are going to need a standard version of a specific software suite (Kepes 2017). Another prime candidate for SaaS usage is for mobile access to a particular set of software (Kepes 2017). SaaS is the cloud computing architectural model which enables the thin client, virtual desktop infrastructure model.

It is sometimes hard to distinguish between the low-level infrastructure and the higher level platform, the line between these two is not always well defined and sometimes are considered the same (Armbrust, et al. 2010, 50). When these two architectural delineations are combined, they comprise the hardware and software that form the cloud (Armbrust, et al. 2010, 51). If these services are offered in a pay as you go format, they comprise a public cloud, if the data centers forming the cloud are owned by an institution, then they comprise a private cloud (Armbrust, et al. 2010, 51).

E. REMOTE DESKTOP PROTOCOLS

So that VPCs can be accessed remotely, a method of transporting the view that is associated with normal computer operations, in particular images on the screen, must be transported via a network to the remote client. At the same time, inputs from the user must be transported from the client back to the VPC. Often, a thin client will be the device that is accessing the VPC remotely. In fact, to maximize the benefits of a VPC, a thin client is ideal for accessing a VPC remotely (Simoens, et al. 2008). By using a thin client, unnecessary hardware can be removed from the client, eliminating excess computing power until all that remains are the limited capabilities of the presentation of the graphical output of the VPC and the ability to capture user inputs at the thin client such as keystrokes and pointer device movements (Simoens, et al. 2008).

In response to the needs created by remote access, Microsoft developed the remote desktop protocol (RDP). RDP was designed to support many differing types of network topologies and capabilities, ranging from plain old telephone service (POTS) and integrated services digital network (ISDN) to high-speed local area networks (LAN) (Microsoft 2014). Sending information over RDP is nearly identical to sending any information through the standard seven-layer open systems interconnection (OSI) model (Microsoft 2014). Data from the application that uses RDP passes down the protocol stack, which travels over port 3389 and through the LAN to and from the VPC and remote client (Microsoft 2014).

Many remote display protocols, including RDP, have been optimized to support applications that do not have large changes to screen images. Spreadsheets, text editors, and general PC usage all works very well with most remote display protocols. Where remote display protocols start to have problems is when high volume, rapid changes are transported (Simoens, et al. 2008). Other competing remote protocols include Citrix's High Definition User Experience (HDX) and Teradici's PC-over-IP (PCoIP) (Kouril and Lambertova 2010, 783). RDP has recently implemented a feature called Aero desktop environment, making it capable of transmitting high definition video without losing synchronization between the audio and the video (Kouril and Lambertova 2010, 783). Similarly, HDX optimized its protocol to utilize bandwidth more efficiently, allowing for

viewing of graphics data through streaming Flash video in its compressed form. Teradici took the optimization a step further, enabling the ability of PCoIP to identify the client device, then select the optimal protocol for data delivery (Kouril and Lambertova 2010, 783).

To show the benefits of using a more optimized remote display protocol, Jiri Kouril and Petra Lambertova (2010) from the Brno University of Technology in the Czech Republic conducted an experiment comparing the performance of RDP compared to PCoIP. Their experiment yielded interesting results, showing that in some instances, such as when only transporting text, RDP far outperformed PCoIP; however, in the category of system response time, PCoIP was much more responsive (785–786).

When setting up the experiment, PCoIP offers far fewer setup parameters than does RDP. The adaptive character of PCoIP contributes to the fewer setup parameters as it senses the network conditions, and adapts to those conditions (Kouril and Lambertova 2010, 784). Figure 5 depicts the results of the bandwidth utilized by RDP. Four Types of traffic are transported by RDP: 1: text, 2: pdf, 3: www, and 4: presentation. Figure 6 depicts the results of the bandwidth utilized by PCoIP. The traffic that overlaps between the RDP and PCoIP experiment are 1: www and 4: presentation. The PCoIP experiment added additional high bandwidth options of 5: Google Earth, 6: Flash Video, and 7: Full HD Video (Kouril and Lambertova 2010, 785).

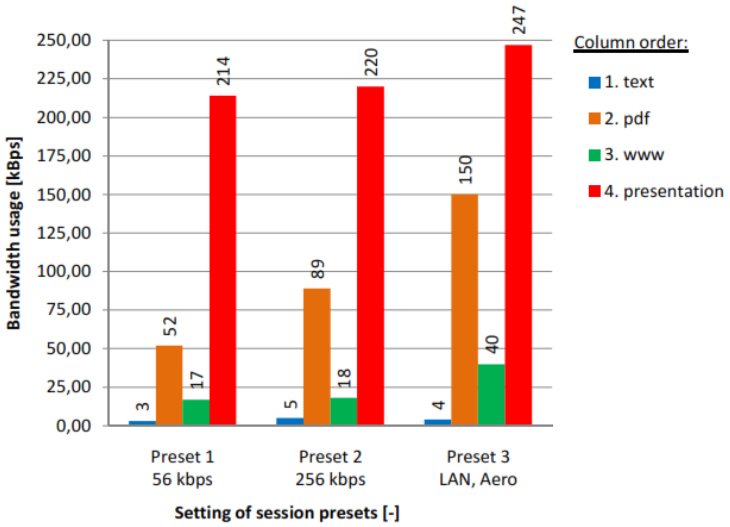

Figure 5. Bandwidth Usage—RDP.
Source: Kouril and Lambertova (2010, 786).

As seen in Figure 6, RDP is an excellent choice when text is the primary data transferred between the client and the VPC. This performance carries over well for pdf files and even more so for standard web traffic, as long as it is primarily text. A noticeable degradation of performance is exhibited when a full multimedia presentation is transferred from the VPC to the client.

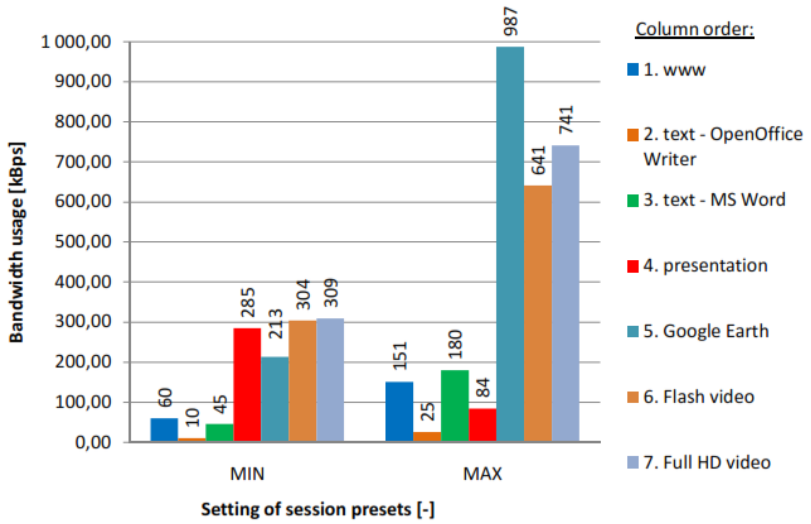

Figure 6. Bandwidth Usage—PCoIP.
Source: Kouril and Lambertova (2010, 786).

When comparing Figure 5 with Figure 6, the bandwidth usage for the lower intensity uses such as text and web traffic, the two protocols perform similarly, with RDP taking a slight performance edge over PCoIP in the min setting. However, RDP greatly outperforms PCoIP when PCoIP utilizes the max setting. Where PCoIP shines is the in the high intensity uses in the constrained min setting. The Google Earth images can transfer in the min constrained setting using less than a quarter of the bandwidth required when PCoIP is given a larger max bandwidth setting. The authors speculate that the reason PCoIP does not perform as well as RDP in many cases is due to the adaptive nature of PCoIP, using as much bandwidth as it can to accomplish the task so as to provide the client with the best possible experience (Kouril and Lambertova 2010, 785).

Another comparison between RDP and PCoIP is in system response time. Here, PCoIP shows that it is a very capable protocol when executing more resource consuming applications. Figure 7 shows the system response time of RDP and Figure 8 shows the system response time of PCoIP. Three applications were compared, and the two protocols were given the same amount of bandwidth and latency. The three applications that were tested were rendering the desktop, browser, and a PDF (Kouril and Lambertova 2010, 786).

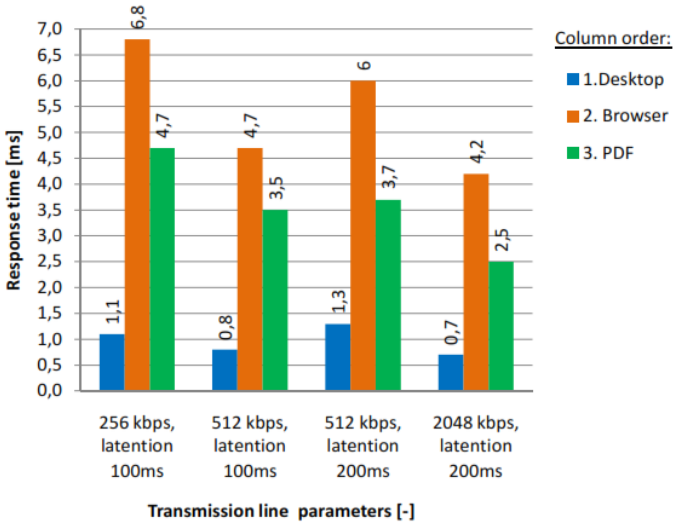

Figure 7. System Response Time: RDP.
Source: Kouril and Lambertova (2010, 786).

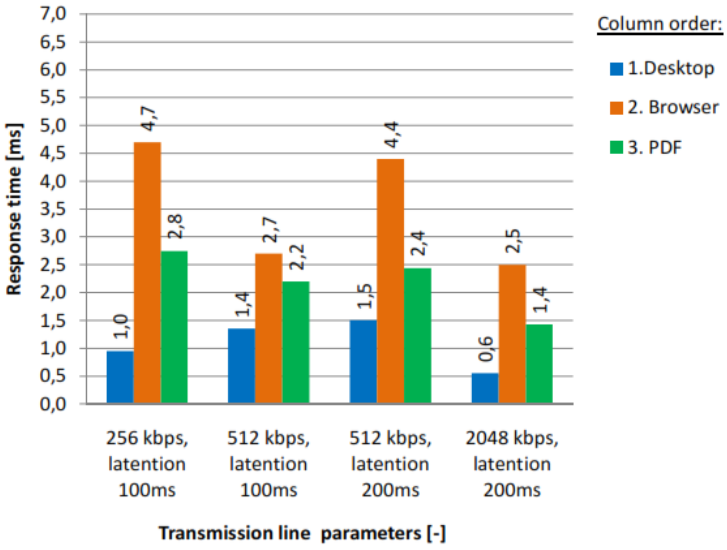

Figure 8. System Response Time: PCoIP.
Source: Kouril and Lambertova (2010, 786).

Once again, when minimal changes in the view are taking place, RDP performs the same or better than PCoIP. The desktop rendering, which is mostly static, is best executed by RDP. However, in the cases where the protocol was not able to store large percentages of unchanging data in the cache, the browser and PDF rendering being prime

examples, the PCoIP protocol provides a better system response time than does RDP (Kouril and Lambertova 2010, 786).

To further improve upon the advantages of adaptive nature of PCoIP, VMware developed a protocol to use as a remote display protocol called Blast Extreme. The Blast Extreme protocol is included with the release of VMware's Horizon 7 remote application-delivery software (Arakelian and Halstead 2016, 3). VMware recommends that the only clients who should continue to use PCoIP instead of the new Blast Extreme protocol are users with thin clients that have been built to specifically support PCoIP (Arakelian and Halstead 2016, 3). Blast Extreme uses one of three codecs to compress and transport desktop images, H.264, JPG, and PNG. The H.264 codec offers large speed advantage for machines that are equipped with NVIDIA graphics processing unit (GPU), as the encoding and decoding are accomplished in hardware instead of software. Browser access via Blast Extreme defaults to the JPG/PNG codec with the exception of Chrome Browsers (Arakelian and Halstead 2016, 3). Chrome has the ability to be configured to use the H.264 codec (Arakelian and Halstead 2016, 3).

VMware claims that Blast Extreme offers many benefits for remote viewing, not the least of which is a very broad client support (Arakelian and Halstead 2016, 4). Through supporting web access, Blast Extreme supports hosts ranging from Windows, Linux, and Mac, to mobile operating systems such as Android and iOS (Arakelian and Halstead 2016, 4). Other benefits are ease of firewall setup and lower energy consumption (Arakelian and Halstead 2016, 4). When setting up a firewall to allow remote access to the virtual machines, only one port has to be opened, port 443. The H.264 codec when decoded with NVIDIA hardware, reduces the load on the device's processor which can prolong battery life on mobile devices (Arakelian and Halstead 2016, 4). The JPG and PNG codecs are used to compress images to transport. It is best used to transport applications such as word processors, which consist of mostly of static content (Arakelian and Halstead 2016, 4). The H.264 codec is a common video encoding format used in Bluray video discs. In contrast to the JPG and PNG codecs, the H.264 encoding and decoding occurs on a GPU, and not the central processor, saving compute cycles and energy use (Arakelian and Halstead 2016, 6).

In addition to multiple encoding codecs, Blast Extreme uses multiple transport protocols. Where PCoIP is only capable of using the user datagram protocol (UDP), Blast Extreme uses both UDP and transmission control protocol (TCP) (Arakelian and Halstead 2016, 4). TCP, because of its end to end connection and error checking, ensures delivery of each packet and that each packet received is error free. UDP does not use these control measures and can transmit information fast, but without the guarantees that TCP affords. UDP is the protocol of choice when the speed of transmission is the most important factor; however, TCP should be used to guarantee the delivery of error free data (Arakelian and Halstead 2016, 5).

F. VIRTUAL PRIVATE NETWORKS

A secure option for remotely accessing a private network is a VPN. VPNs emulate private secure data networks over generally insecure shared facilities (Sheneyderman and Casati 2003, 4). Sheneyderman and Casati define VPNs as combining two concepts, virtual networking and private networking. (2003, 138) By using virtual networking, "geographically distributed and remote nodes can interact with each other the way they do in a network where the nodes are collocated" (Sheneyderman and Casati 2003, 4). Virtual networking separates the physical topology from the logical topology. A private network is a network that is implemented on private, or non-shared networking facilities, consisting of hosts and clients belonging to the same company or administrative entity (Sheneyderman and Casati 2003, 138). The term VPN was first used by phone companies but did not actually provide privacy. It was a method to provide software defined user groups a set of services; however, as IP grew, VPNs expanded through Cisco and Microsoft leading to VPN technologies such as IPSec and L2TP (Sheneyderman and Casati 2003, 8–9).

Sheneyderman and Casati (2003) break VPNs down into five fundamental building blocks: "access control, authentication, security, tunneling, and service level agreements" (138–141). They then define access control as "a set of policies and techniques governing access to the private networking resources for authorized parties" (141). Additionally, they make an important note, with regards to access control, is that it

is separate and independent from authentication (2003, 138–141). Authentication is used to ensure that the entities involved in communication on the VPN can positively identify themselves to each other, providing mutual authentication. Mutual authentication can be accomplished with symmetric methods such as a pre-shared key or using asymmetric methods such as the public key infrastructure (Sheneyderman and Casati 2003, 144). Security is composed of two elements, data integrity and encryption. Encryption is the process by which the information transmitted over the VPN is converted into a code to prevent unauthorized access. Integrity ensures that no alteration to the data has occurred and the data is being transmitted from a legitimate source (Sheneyderman and Casati 2003, 144). Tunneling is the "encapsulation of certain data packets within other packets according to a set of rules implemented at both ends of a tunnel" (Sheneyderman and Casati 2003, 145). Encapsulation results in the contents of the encapsulated packets becoming obfuscated to unauthorized observers (Sheneyderman and Casati 2003, 145). Tunneling is considered to be the "most important technology on which IP VPNs are built" (Sheneyderman and Casati 2003, 145). Tunnels are defined by the end points of the tunnel and the tunneling protocol being used. By using tunnels, three major tasks of VPNs are accomplished. The data is encapsulated becoming unobservable, it is possible to use private IP address space and routed over the public IP space, and ensure end-to-end integrity and confidentiality of data (Sheneyderman and Casati 2003, 146). The final building block of VPNs is the service level agreements, these are the business considerations of a VPN and are concerned with things such as service levels and revenues. These agreements are made between the entities involved in the VPNs such as wireless carriers, Internet service providers, and the remote users utilizing VPNs (Sheneyderman and Casati 2003, 149).

There are three main VPN architectures: site to site, intranet, and remote access. A "site-to-site VPN is used to connect geographically distributed corporate sites, each with private network addresses administered in such a way that normally conflicts do not arise" (Sheneyderman and Casati 2003, 156). An intranet VPN is used to "establish and manage different levels of internal access to specific information," creating "an environment similar to physically segmenting groups of users on distinct LAN subnets"

(Sheneyderman and Casati 2003, 159). Remote access VPNs "provide remote hosts with access to information resources and data services located in a private network" (Sheneyderman and Casati 2003, 159).

G. CHAPTER SUMMARY

This chapter outlined the technology that is currently in use to support GCSS-MC. Additionally, it shows some of the challenges that the users of GCSS-MC face, especially mobile users. It also discussed the technology to enable mobile access to GCSS-MC without changing the architecture or features of GCSS-MC. The ability to remotely access GCSS-MC with any device is possible with the combination of VPCs and a VPN. Chapter III offers a proof of concept framework that enables an OS agnostic, mobile, and remote access solution.

III. EXPERIMENTAL DESIGN

This chapter outlines the experiment that is performed to show a technologically sound framework offering an OS agnostic, mobile, and remote access solution for GCSS-MC. It details the tools, hardware, and network utilized during experimentation. The chapter then sets up the experimentation by providing information for the database utilized during testing, the SQLs that run against the database, and finally the data collection methods used during the experiment.

A. TOOLS UTILIZED IN EXPERIMENTATION

Several tools are utilized for evaluating the use of VPCs as a technologically viable method to access GCSS-MC remotely. The primary tools range from the remote desktop viewer to a packet capture analyzer. A summary of each tool is in this section, with the pertinent application and employment details outlined.

1. VNC Connect Viewer

The remote desktop viewer used during experimentation is the RealVNC Connect Viewer. This application is available for Windows, Mac OS X, Linux, Raspberry Pi, Android, iOS, Chrome and more. Connect Viewer uses the remote framebuffer (RFB) protocol for remote access to the VPC (REALVNC 2016). RFB is designed to be a thin client protocol and minimizes the amount of information exchanged between the client and the VPC server. Additionally, RFB makes the client stateless, meaning that state of all running applications is maintained at the server, not the client, making the interface between the client and the server completely mobile (Richardson 2011).

Security in VNC Connect is taken seriously; all data in transit is encrypted using AES-GCM for integrity and security. The standard version of VNC Connect uses 128-bit AES encryption with the option of upgrading to 256-bit encryption in the Enterprise solution. In addition to the security in transit, VNC Connect makes use of identity checking to ensure that the client knows that it is connecting to the appropriate server preventing impersonation. An RSA key identifies each client, and Elliptic Curve Diffie-

Hellman key exchange is used to ensure perfect forward secrecy for each connection (REALVNC 2016).

2. Keuwlsoft Wi-Fi Analyzer

The Wi-Fi Analyser by Keulsoft is used to ensure that the Wi-Fi connection is strong enough to conduct the testing throughout the experimentation. The Wi-Fi analyzer was run on the Samsung Galaxy S5 Active to measure signal strength and speed. The Wi-Fi analyzer measures several variables, the Received Signal Strength Indication (RSSI), link speed, channel, and network ID. The RSSI is measured in dBm and records the maximum, minimum, and average values. Primarily this tool is intended to help users to place wireless devices in areas where signal strength is strong enough to function properly (Keuwlsoft 2017). Figure 9 shows an example output of the Wi-Fi analyzer.

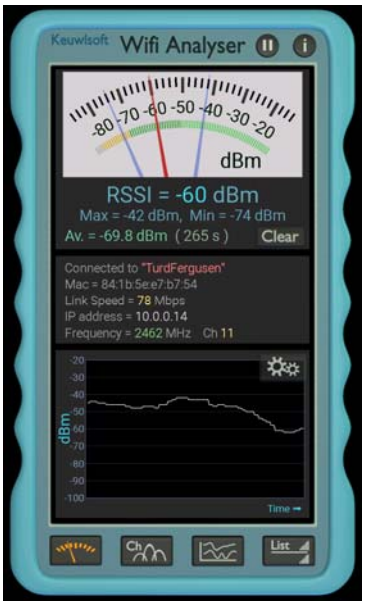

Figure 9. Example Output of Wi-Fi Speed Analyzer.
Source: Keuwlsoft (2017).

The RSSI and the link speed are the two most relevant items that the Wi-Fi Analyzer provides. The RSSI is the signal strength of the Wi-Fi network that the device is measuring. The RSSI is measured in dBm, the lower the indicated number, the better the signal strength. The link speed is also very relevant to testing. As potentially the slowest

link in the equipment string between the device being used to access the VPC or database, the Wi-Fi link must be properly analyzed to ensure a sufficient link speed and signal strength.

3. Ookla SpeedTest

The Ookla SpeedTest is utilized to measure Internet speeds from the various devices and the various locations. When being measured from the PC, the Ookla SpeedTest measures through the PC's browser. Additionally, for mobile devices, Ookla offers applications in the Apple App Store, Amazon Apps, Google play, and the Windows Store. The version for iOS and Android were installed on the mobile devices used in the testing phase. Figure 10 depicts sample output of the both the desktop and mobile versions of Ookla SpeedTest.

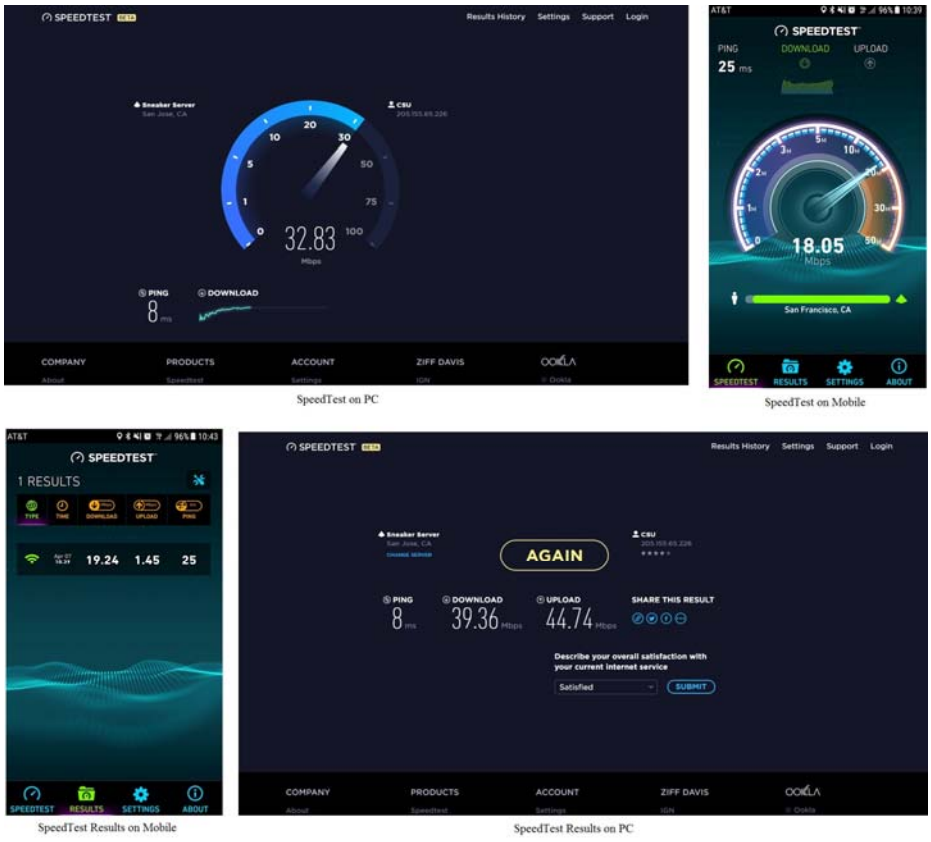

Figure 10. Network Speed Testing and Results—Desktop and Mobile. Source: Ookla (2017).

The SpeedTest application allows the user to select which server to use to test the connection speed. The three factors that are measured by SpeedTest are ping, download speed, and upload speed. The ping test measures the latency between the user system and the server. The ping test is conducted multiple times with the fastest time reported (Ookla 2017). The download speed is measured by establishing up to four connections over port 8080 and sending data from the server to the client. The number of threads used is determined during the pre-test, if the speed is determined to be four megabits per second, four threads will be used, otherwise, two are used. Once chunks of data are received from the server, more data is requested by the client system with the client calculating the real time speed of the transfers. The upload test is conducted in a similar manner, with the data flowing from the client to the server over the defined port and multiple connections being utilized to determine if additional threads are required to accurately measure the speed (Ookla 2017).

4. Wireshark

Wireshark is a widely used network protocol analyzer that allows deep packet inspection of hundreds of protocols. Wireshark can capture live traffic and has the ability to analyze traffic captures offline. Wireshark can capture traffic over many types of signals, including but not limited to Ethernet, Wi-Fi, Bluetooth, and USB (Wireshark 2016). For experimentation purposes, this tool is used to capture the traffic between the Lenovo workstation and the VPC, as well as the traffic between the Lenovo workstation and the GCSS-MC Tables database. One of the most useful tools offered by Wireshark during offline analysis is the display filters. Wireshark's display filters allow for the isolation of packet flows with coarse filters to a particular source or destination IP addresses, or granular filters such as flows to individual ports on those IP addresses. Figure 11 shows a packet capture and Wireshark's standard three-pane browser used to inspect a packet capture (Wireshark 2016).

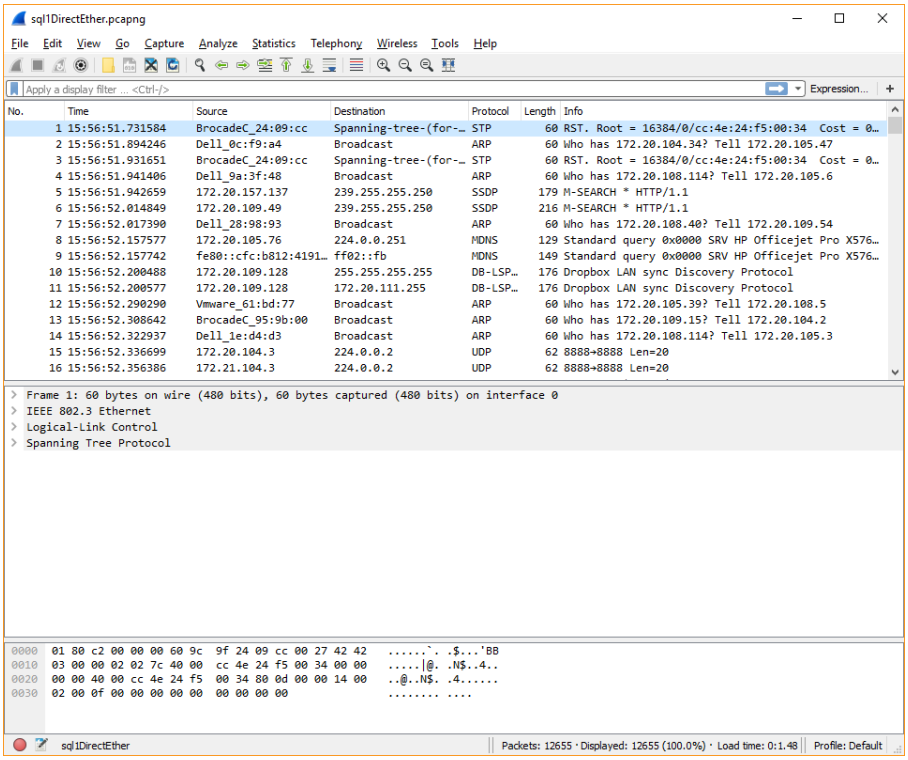

Figure 11. Wireshark Packet Capture. Source: Wireshark (2016).

5. SQL Developer

SQL Developer, an integrated development environment designed for use with Oracle databases, is a free tool that enables database users and administrators to interact with and manage Oracle databases. SQL Developer is designed to run on any system that supports Java and provides an editor for writing SQL, running queries, and exporting data in multiple formats ranging from XML, Excel or HTML (Oracle 2015). Specifically, in the case of experimentation, SQL developer is used as a stand-in for and to simulate the E-Business Suite. Figure 12 shows the work environment experienced when using SQL developer regardless of the device using to access it during experimentation.

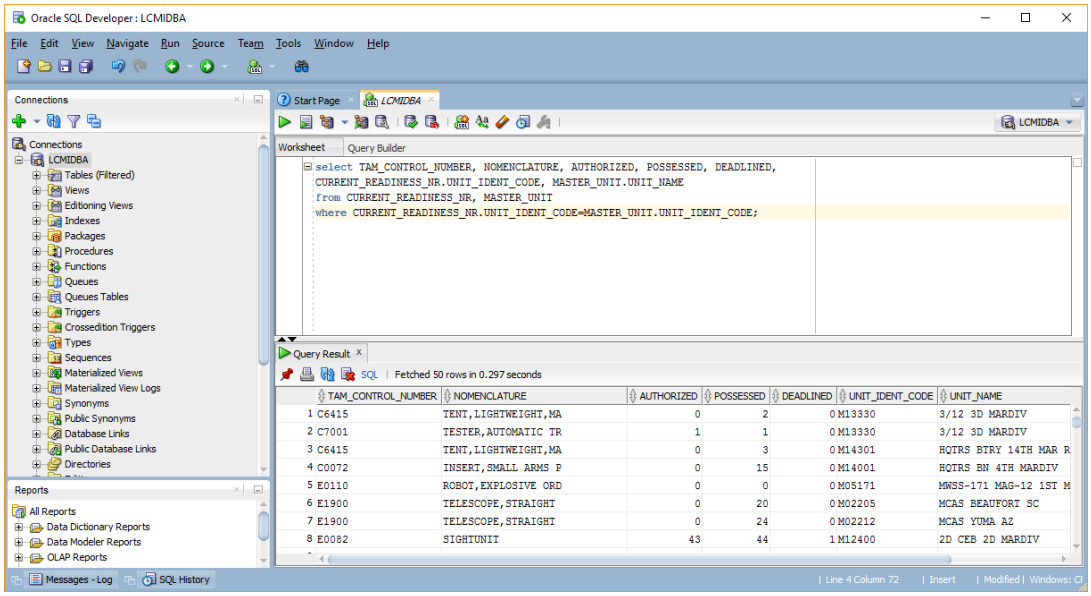

Figure 12. SQL Developer Environment. Source: Oracle (2015).

B. HARDWARE UTILIZED IN EXPERIMENTATION

In this section all hardware used in the experimentation is described, along with performance and detailed specifications. For experimentation purposes, all devices are mobile capable platforms. A Windows laptop, an Android smartphone, an Android tablet, and an Apple tablet are used to cover the range of devices in popular use today.

1. Lenovo Laptop

The primary workstation utilized for the experimentation is a Lenovo G50-45. Lenovo G50-40 is a budget, consumer-grade laptop with few additions or upgrades. The Lenovo workstation has a 15.6-inch High Definition screen, a full-size keyboard with a dedicated number pad and a traditional touchpad with dedicated mouse buttons. Table 1 summarizes the performance and hardware specifications for the workstation.

Table 1. Lenovo G50-45 Specifications

Operating System	Windows 10 Home Edition
Processor	AMD A8-6410 APU
Processor Cores	4
Processor Speed	2.0 GHz
Memory	16 GB
Wi-Fi Adapter	Realtek RTL8723BE 802.11n PCI-E Network Interface Card
Ethernet Adapter	Realtek PCIe GBE Family Controller

2. Samsung Galaxy S5 Active

The Android smartphone utilized for the experimentation is a Samsung Galaxy S5 Active. Galaxy S5 Active is a ruggedized version of the standard Galaxy S5. When new, the S5 was Samsung's flagship device; however, as it is three generations old now, it offers a more budget device level of performance. The Galaxy S5 Active has a 5.1-inch active-matrix organic light emitting diode high definition screen. Of the three mobile devices tested (described in the following sections), the Galaxy S5 Active had the highest performance specifications. Performance and hardware specifications for the Galaxy S5 Active are summarized in Table 2.

3. Samsung Galaxy Tab 4

Samsung Galaxy Tab 4 represents the Android tablet market for our experimentation purposes. Tab 4 has a 7-inch high definition thin film transistor capacitive touchscreen. Tab 4 represents consumer grade electronics and does not have any of the ruggedized features found in S5 Active. Tab 4 also operates on an older version of Android and is not as high powered as the Galaxy S5 Active; however, it is substantially equipped to operate the VPC remotely for experimentation purposes. Table 2 summarizes the performance and hardware specifications for the Galaxy Tab 4.

4. Apple iPad Mini

Apple iPad mini has an in-plane switching, liquid crystal display capacitive touchscreen. Similar to Tab 4, iPad mini represents consumer grade electronics and does not have any of the ruggedized features found in the S5 Active. iPad mini is the lowest

powered device tested but is still fully capable of operating the VPC remotely for experimentation purposes. Table 2 summarizes the performance and hardware specifications for iPad Mini.

Table 2. Mobile Device Specifications

	Galaxy S5 Active	Galaxy Tab 4	iPad Mini
Operating System	Android 6.0.1	Android 4.4.2	iOS 9.3.5
Processor	Snapdragon 801	Marvell PXA1088	Apple A5
Processor Cores	4	4	2
Processor Speed	2.5 GHz	1.2 GHz	1.0 GHz
Memory	2 GB	1.5 GB	0.5 GB
Wi-Fi Type	802.11 a/b/g/n/ac	802.11 a/b/g/n	802.11 a/b/g/n

5. Virtual PC

The VPC used for testing is hosted on a Dell Power Edge 620 Server on the Naval Postgraduate School Campus. Initially, a Windows VPC hosted by the Naval Postgraduate School Cloud Labs was to be used, but difficulties in running SQL developer on a workstation running DOD security policies proved prohibitive. A VPC running a Linux operating system was settled on due to its compatibility and availability. Table 3 summarizes the virtual specifications and physical specifications of the VPC and the server hosting the VPC.

Table 3. Virtual PC Specifications

Operating System	Linux 2.6.32-642.13.1 (Red Hat)
Processor (Virtual)	Intel Xeon E5-2665
Processor Cores (Virtual)	2
Processor Speed (Virtual)	2.4 GHz
Memory (Virtual)	3.7 GB
Processor (Physical)	2 x Intel Xeon CPU E5-2665
Processor Cores (Physical)	9 per Processor
Processor Speed (Physical)	2.4 GHz
Memory (Physical)	384 GB

6. The VPN

The Naval Postgraduate School enterprise network utilizes Cisco AnyConnect Secure Mobility Client. The software to operate the AnyConnect VPN is available for a wide variety of devices including Windows, MacOS, iOS, Android, Google Chrome OS, and Amazon Kindle. As well as being available to a wide range of devices, AnyConnect supports strong encryption including AES-256 and 3DES-168. Authentication is available through many options including remote authentication dial-in user service (RADIUS), RADIUS with password expiry, RADIUS one-time password, Active Directory, Digital Certificates, multifactor authentication, and others (Cisco 2016). The Naval Postgraduate School network makes use of the username and password RADIUS option. While Cisco AnyConnect supports split-tunneling, the Naval Postgraduate School policy does not support this option (Cisco 2016). Cisco claims that the AnyConnect VPN optimizes network access because it "adapts its tunneling to the most efficient method possible base on network conditions" (Cisco 2016). Making further claims as to optimized network access, AnyConnect is "compatible with adaptive security appliance VPN load balancing" (Cisco 2016).

C. NETWORK UTILIZED IN EXPERIMENTATION

The network utilized to during testing is the Naval Postgraduate School campus network. The campus network represents the MCEN for experimental purposes. There are specific portions of the network that are utilized during different phases of testing. As the network can be a large variable in the testing, each equipment string for each phase of testing is documented and analyzed.

When accessing the database from the campus network with the Lenovo workstation, there are two options. Option one is to go directly through the hardwired Ethernet LAN, and option two is to access the LAN through the Wi-Fi. Both options are tested during experimentation. Figure 13 depicts the equipment string of the Ethernet LAN and Figure 14 depicts the equipment string of the Wi-Fi LAN to access the database being tested. These two equipment strings represent direct manipulation of the database from the Lenovo workstation.

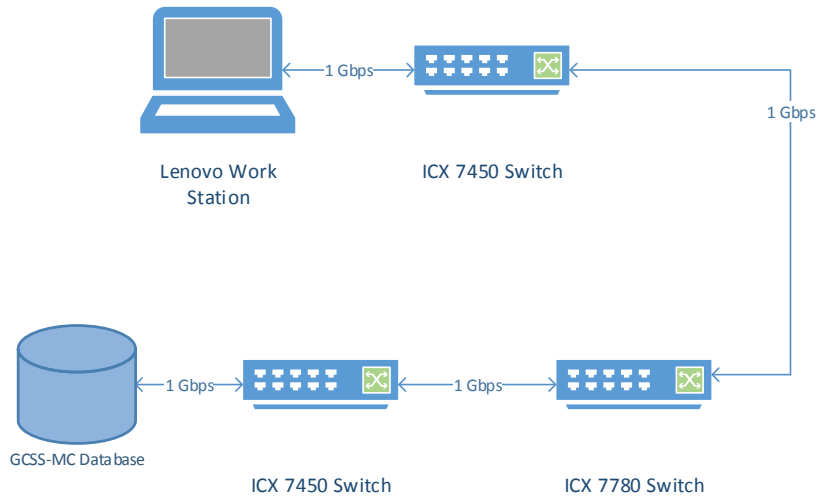

Figure 13. Ethernet Equipment String Workstation to Database

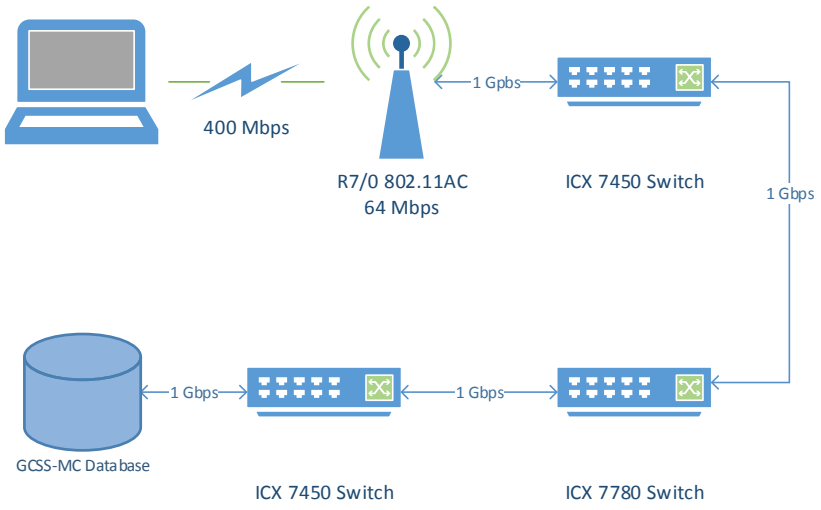

Figure 14. Wi-Fi Equipment String Workstation to Database

Access to the VPC through the Wi-Fi LAN was tested from the Lenovo workstation as well as all of the mobile devices. The same Wi-Fi access point is used for testing each device's access to the VPC. Figure 15 depicts the equipment string from each of the mobile devices and the Lenovo workstation to the server hosting the VPC.

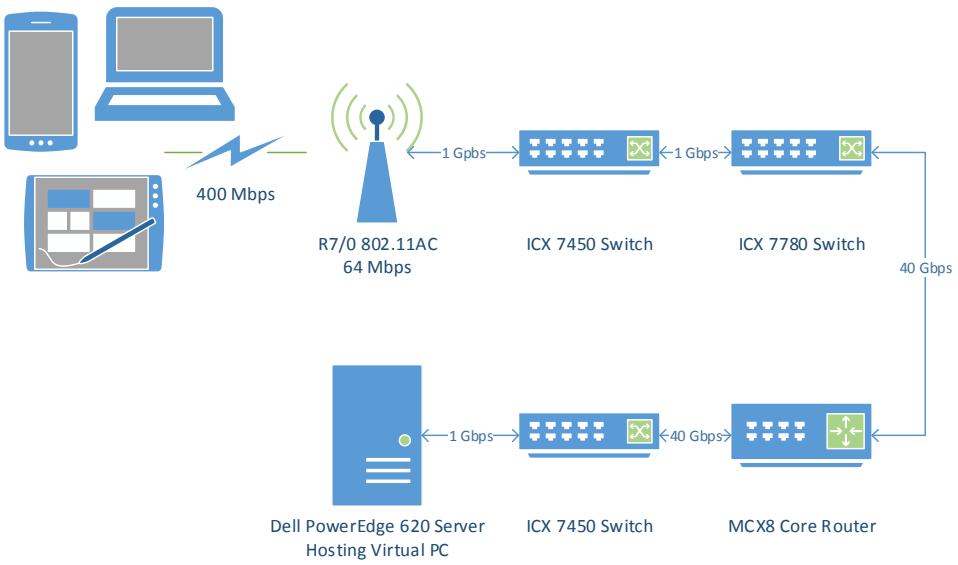

Figure 15. Wi-Fi Equipment String All Devices to VPC

In addition to testing the VM accessing from the Lenovo workstation from the Wi-Fi, the wired LAN was tested as well. The wired LAN was tested to allow a comparison of speeds accessing the VPC from both Wi-Fi and Ethernet. Figure 16 depicts the equipment string from the Lenovo workstation to the server hosting the VPC through the wired LAN.

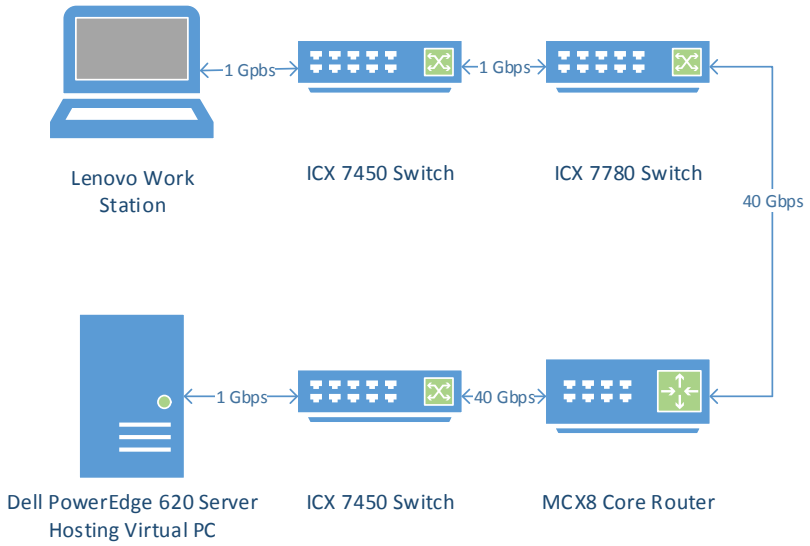

Figure 16. LAN Equipment String Lenovo Workstation to VPC

Access to the VPC is the first half of accessing the database. Once the device being tested accesses the VPC, the VPC then has to access the database. As when accessing the database directly, SQL developer is used to access the database. SQL developer is run on the VPC which then access the database through the LAN. The database is hosted on the Naval Postgraduate School campus on a Dell 2850 4U server with two dual core Intel Xeon processors operating at 2.66 GHz, 48 GB of RAM and 222 GB or disk space. Figure 17 depicts the equipment string from the server hosting the VPC to the database.

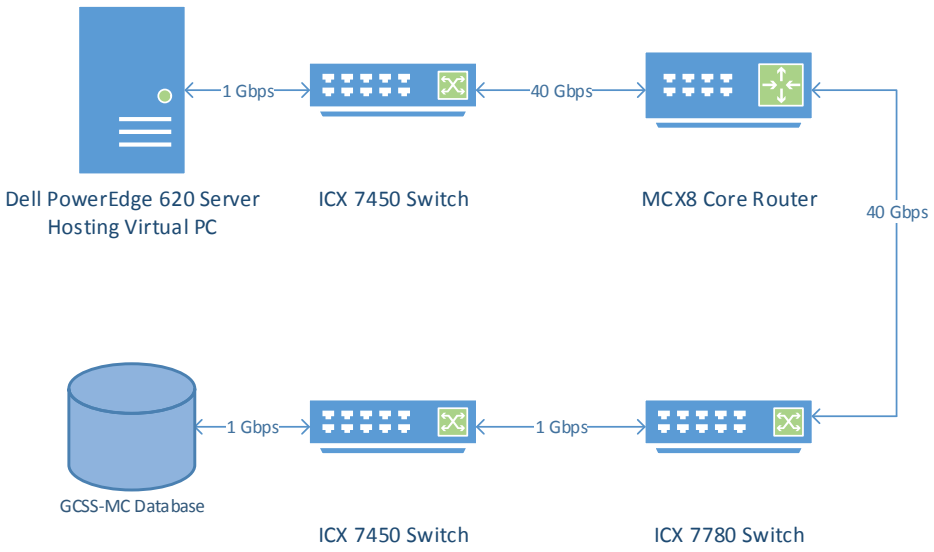

Figure 17. LAN Equipment String VPC to Database

The final equipment strings that are utilized during the testing make use of a VPN to remotely access the campus LAN. This portion of the testing utilizes the VPN to replicate remote access of GCSS-MC from off of the MCEN. Two methods of accessing the database were tested remotely. Figure 18 depicts direct access to the database, and Figure 19 depicts access from the VPC.

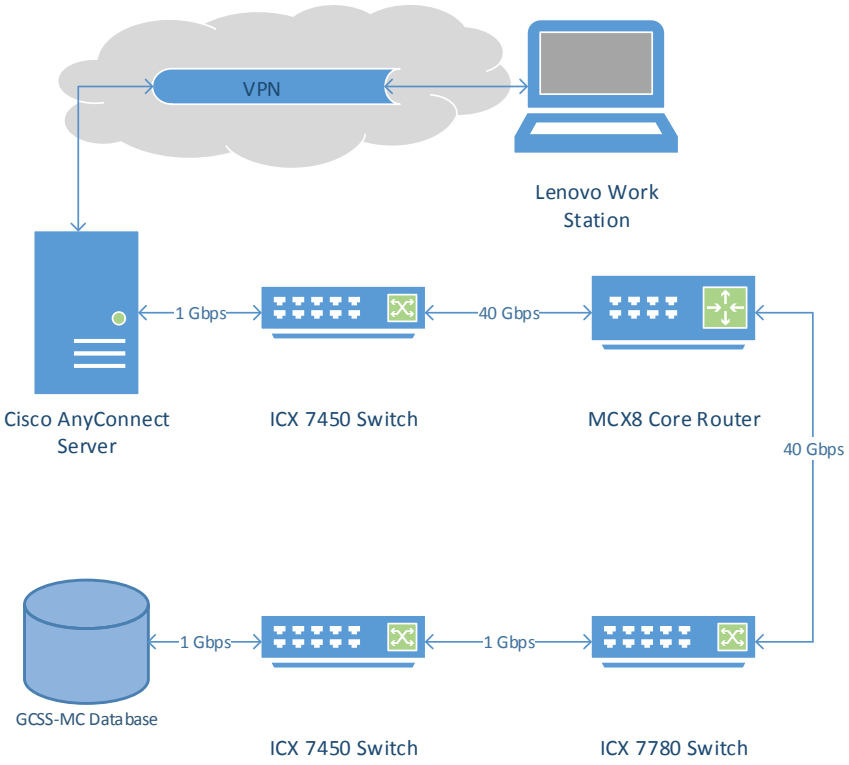

Figure 18. VPN Equipment String Lenovo Workstation to Database

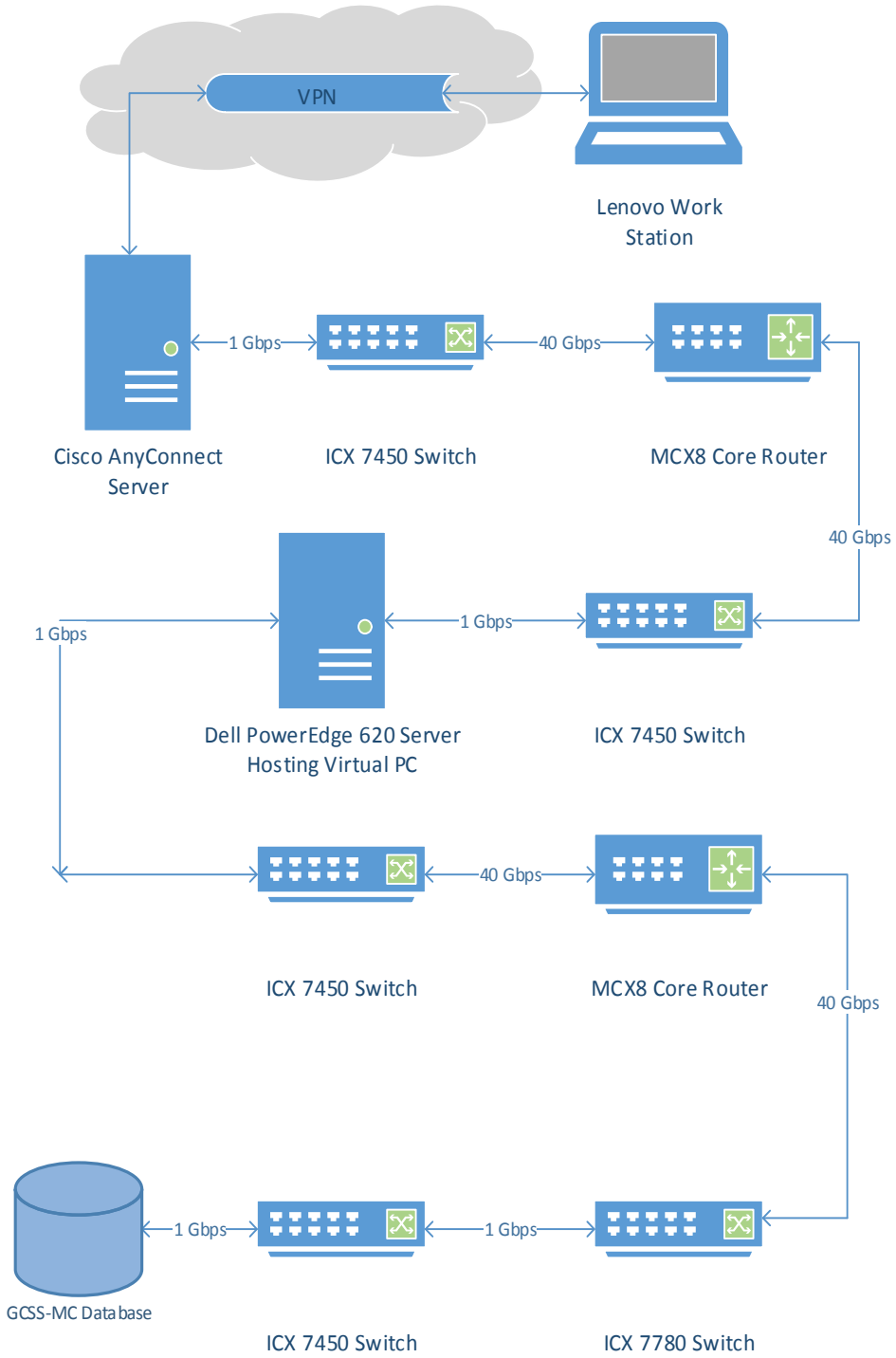

Figure 19. VPN Equipment String Lenovo Workstation to VPC

D. GCSS-MC TABLES

A database server hosting a 2014 snapshot of GCSS-MC is hosted on the campus of the Naval Postgraduate School. The GCSS-MC Tables is the database on which the experimentation is being conducted. This data was provided by the Marine Corps so that big data analysis could be conducted on the data. This effort is still ongoing by other members; however, as the data is available and offers a great insight as to how the data of GCSS-MC is organized and allows us to conduct the experimentation. The Naval Postgraduate School does not possess the Oracle E-Business Suite, and GCSS-MC Tables database, along with the SQL developer, serve as the stand-in for the E-Business Suite for experimentation.

By using the Oracle built-in analytic table, ALL_TABLES, the GCSS-MC Tables database contains 403 different tables. Many of these tables, 92 of them, are system tables which are used in the background to manage the database. When the systems tables are accounted for, the remaining 311 tables are actual data tables to conduct our analysis. The tables greatly vary in size, some containing as few as two rows, and the largest data table containing 1,683,089,427 rows. All told, this database occupies roughly six gigabytes on the database server and gives sufficient data for analysis of a snapshot of GCSS-MC.

E. TEST SQLS

Further analysis of the GCSS-MC Tables allowed for focusing in on tables that were large enough to provide meaningful returns from the queries. The small tables that only contained two rows would not provide very much in the way of returning large amounts of data. At the same time, a table with 1.6 billion rows may provide too big of a return if a select * were performed on it. By further analyzing ALL_TABLES a total of eight table were identified for the experimentation. Table 4 summarizes the tables used in testing and their attributes. The tables were chosen to give a varying table size with the smallest table only 639 rows and the largest tables over 140,000 rows.

Table 4. Tables Utilized During Experimentation

Table Name	Rows	Avg Row Length (Bytes)
DASF_UNIT_LEVEL	144,412	188
CURRENT_READINESS_NR	85,606	163
MASTER_UNIT	639	73
CURRENT_OPEN_PARTS_ON_ORDER	141,925	116
CURRENT_OPEN_EROS	64,913	109
CURRENT_DEADLINED	6,613	109
TAMCN_DIM	12,563	38
CURRENT_READINESS	14,714	241

SQLs were chosen to provide returns that would join varying numbers of tables and rows. Each of the SQLs was chosen so that a large number of rows were returned, with the lowest number of rows being 85,606 rows and the largest being 144,412 rows. Table 5 contains the attributes of each SQL used during testing.

Table 5. Test SQLs

Name	SQL	Rows
SQL1	select DOCUMENT_NUMBER_REQ, DOCUMENT_NUMBER_JUL_DT, DOCUMENT_NUMBER_SRL_NUM, RECORD_FED_STOCK_NUMBER, UNIT_QUANITY_BACK_ORDER, QUANTITY_DUE, QUANTITY_RECEIVED from DASF_UNIT_LEVEL;	144,412
SQL2	select TAM_CONTROL_NUMBER, NOMENCLATURE, AUTHORIZED, POSSESSED, DEADLINED, CURRENT_READINESS_NR.UNIT_IDENT_CODE, MASTER_UNIT.UNIT_NAME from CURRENT_READINESS_NR, MASTER_UNIT where CURRENT_READINESS_NR.UNIT_IDENT_CODE = MASTER_UNIT.UNIT_IDENT_CODE;	85,606
SQL3	select CURRENT_OPEN_EROS.OWNING_UIC, UNIT_NAME, CURRENT_OPEN_PARTS_ON_ORDER.TAMCN, CURRENT_OPEN_EROS.ERO, CURRENT_OPEN_PARTS_ON_ORDER.RECORD_NSN from CURRENT_OPEN_PARTS_ON_ORDER, CURRENT_OPEN_EROS, MASTER_UNIT where CURRENT_OPEN_PARTS_ON_ORDER.TAMCN = CURRENT_OPEN_EROS.TAMCN and CURRENT_OPEN_PARTS_ON_ORDER.ERO = CURRENT_OPEN_EROS.ERO and CURRENT_OPEN_EROS.OWNING_UIC = MASTER_UNIT.UNIT_IDENT_CODE;	132,983
SQL4	select CURRENT_DEADLINED.OWNING_UIC, UNIT_NAME,	114,339

Name	SQL	Rows
	CURRENT_DEADLINED.TAMCN, TAMCN_NOMEN, CURRENT_OPEN_PARTS_ON_ORDER.RECORD_NSN, CURRENT_OPEN_PARTS_ON_ORDER.QUANTITY_REQUIRED from CURRENT_DEADLINED, TAMCN_DIM, MASTER_UNIT, CURRENT_OPEN_PARTS_ON_ORDER where CURRENT_DEADLINED.TAMCN = TAMCN_DIM.TAMCN and CURRENT_DEADLINED.OWNING_UIC = MASTER_UNIT.UNIT_IDENT_CODE and CURRENT_DEADLINED.ERO = CURRENT_OPEN_PARTS_ON_ORDER.ERO;	
SQL5	select CURRENT_DEADLINED.OWNING_UIC, MASTER_UNIT.UNIT_NAME, CURRENT_DEADLINED.TAMCN, TAMCN_NOMEN, AUTHORIZED, POSSESSED, DEADLINED, CURRENT_OPEN_PARTS_ON_ORDER.RECORD_NSN, CURRENT_OPEN_PARTS_ON_ORDER.QUANTITY_REQUIRED from CURRENT_DEADLINED, TAMCN_DIM, MASTER_UNIT, CURRENT_OPEN_PARTS_ON_ORDER, CURRENT_READINESS where CURRENT_DEADLINED.TAMCN = TAMCN_DIM.TAMCN and CURRENT_DEADLINED.OWNING_UIC = MASTER_UNIT.UNIT_IDENT_CODE and CURRENT_DEADLINED.ERO = CURRENT_OPEN_PARTS_ON_ORDER.ERO and CURRENT_DEADLINED.OWNING_UIC = CURRENT_READINESS.UNIT_IDENT_CODE and CURRENT_DEADLINED.TAMCN = CURRENT_READINESS.TAM_CONTROL_NUMBER;	106,162

When choosing the varying SQLs, the fields should be indicative of something that a supply clerk may be query of GCSS-MC. SQL1 was chosen to access only one table, DASF_UNIT_LEVEL, and return a large number of rows with seven fields. The Fields represented the common usage items such as the document number, date, serial number of parts on order, the national stock number, quantity of items on back order, the quantity of that item that is due to be delivered and how many of that item that has been delivered. SQL2 accesses two separate tables, linking the unit identifier code (UIC) in the CURRENT_READINESS_NR table to the actual unit name located in the MASTER_UNIT table. SQL3 accesses three tables, continuing to link the UIC with the unit name, and further linking the document number associated with open equipment repair order (ERO) with the parts that are on order. SQL4 accesses four tables and continues to build on SQL2 and SQL3, adding links to dead lined pieces of equipment, with the equipment's name, the unit that owns the equipment, and what parts are on order

to fix the deadlined equipment. SQL5 accesses five tables, once again linking unit names to the UIC, dead lined end items, the end item's name, with quantities authorized, possessed, and parts on order for the dead lined end items.

F. EXPERIMENTATION

This section outlines what is tested during the experimentation and the methodology of testing. Experimentation begins first by analyzing the Wi-Fi coverage and Internet speed to baseline the testing. Once Internet and Wi-Fi baselining is complete, the SQLs are tested. First, from the hardwired Ethernet available on the Naval Postgraduate School campus, the SQLs are run directly from SQL developer; then they are repeated over the Wi-Fi. Next, the SQLs are run using the VPC accessed from the Lenovo workstation both on Wi-Fi and Ethernet. The SQL testing continues by executing the SQLs via the VPC utilizing the mobile devices. Finally, the experiment is repeated remotely accessing the Naval Postgraduate School network using a VPN.

1. Wi-Fi Coverage Analysis

The Naval Postgraduate School campus Wi-Fi, NPS Wireless, is tested using the Keuwlsoft Wi-Fi analyzer. The Wi-Fi signal strength is measured at various times throughout the day to ensure that Wi-Fi coverage did not drop or surge throughout the day. The analyzer was run for five minutes to obtain maximum, minimum and average signal strengths at 0830, 1000, 1130, 1300, 1430, and 1600. This testing is conducted in the same location throughout experimentation. A steady Wi-Fi signal is imperative to testing accuracy.

2. Internet Speed Testing

Similar to the Wi-Fi coverage analysis, Internet speeds play a crucial role in testing accuracy. The Ookla SpeedTest is used to test each device's ability to access the Internet and the speed at which it can access. The Internet speeds are measured from each device twice throughout the day: once in the morning at 0900, and again in the afternoon at 1500. During both the morning and evening tests, the SpeedTest is run ten times from

each of the devices to establish a minimum, maximum, and average values from the Ping, Upload, and Download tests.

3. SQL Testing

Once baseline Internet coverage has been established, the bulk of the testing begins. The first step in testing the SQLs is to directly run the queries with SQL Developer over the hardwired Ethernet using the Lenovo workstation. Each of the five SQLs is run ten times, recording the time to retrieve all of the data by executing the desired query. On the first run of each of the SQLs, Wireshark is run to capture the traffic data. When the SQL testing over the hardwired Ethernet is complete, the same steps are completed using the campus Wi-Fi. Each of the five SQLs is run ten times from SQL developer, recording the time to retrieve all of the data from executing the query. Wireshark is run again during the first run of each SQL to capture the traffic data.

The next step in testing the SQLs is to run them utilizing the VPC. The VPC is accessed through the Lenovo workstation. Similar to the previous testing, the first round of testing using the VPC is over the hardwired Ethernet. Each of the five SQLs is run ten times, recording the time to retrieve all of the data from executing the query. On the first run of each of the SQLs, Wireshark is run to capture the traffic data. The final step utilizing the Lenovo workstation is to access the VPC over the campus Wi-Fi. Just as in all of the previous rounds of testing, each of the five SQLs is run ten times using the VPC over the campus Wi-Fi with Wireshark capturing traffic data on the first run of each of the five SQLs.

Having established a baseline of operations utilizing the Lenovo workstation, the mobile devices now have to be tested. Unlike the Lenovo workstation, the mobile devices do not have an RJ45 connector; the mobile devices are only tested over Wi-Fi. However, identical to the testing using the Lenovo workstation, the mobile devices are used to access the VPC.

4. Remote Location Testing Utilizing a VPN

The next step in testing is to move off of the campus and utilize the VPN to access the database remotely. Residential Internet provided by AT&T is utilized, which does not have the same speed capabilities as the campus network. While testing on campus replicates mobile access from inside the MCEN, utilizing the VPN would provide remote access from outside of the MCEN. Similar to on-campus testing, an Internet speed baseline is the first thing that is established. Again utilizing the SpeedTest, Upload, Download and Ping tests are recorded ten times. The speed test was conducted after connecting to the VPN, showing the actual speeds experienced at the workstation when capable of accessing the database and VPC.

After establishing the speed of the available Internet, the SQLs are again tested. Just as in the previous testing, SQL developer is first used to execute the five SQLs ten times each, connecting directly to the database and recording the execution time to retrieve all of the data produced by the SQLs. Wireshark is again used to capture traffic data on the first run of each of the five SQLs. The final testing conducted is using the Lenovo workstation to access the VPC and run the same five SQLs ten times. Finally, the Lenovo workstation is connected to the VPC, and each of the five SQLs is run ten times, collecting traffic data on the first run of each SQL using Wireshark.

G. CHAPTER SUMMARY

Chapter III reviews the tools and software used to measure performance metrics and conduct the testing. Furthermore, this chapter outlines the hardware utilized in experimentation and the associated performance specifications. The chapter then details the network used for testing before discussing the SQL queries that are executed during testing. Finally, the chapter III details the procedures that are used for the testing, ranging from the SQL queries directly to the database to accessing the VPC from a VPN at a remote location. Chapter IV addresses the results of the testing outlined that are outlined in Chapter III.

IV. TESTING AND RESULTS

This chapter details the results of the experiments outlined in Chapter III. It begins with first testing the Wi-Fi coverage of the network that is used later in the tests. The connection speeds of the available network are then tested, recording the ping response time, upload speed, and download speed from each of the devices used during testing. The SQLs are then run against the database to collect time of execution and throughput information using a direct connection to the database server with SQL Developer, as well as the mobile devices ability to access the VPC and execute the same SQLs through the VPC. Finally, the ability to access the database through a VPN is tested, utilizing both a direct connection and the VPC.

A. WI-FI COVERAGE

To ensure that the Wi-Fi coverage is sufficient to execute the experiment, the Keuwlsoft Wi-Fi analyzer is used to measure the connection speed and signal strength. The signal strength is measured throughout the day to make sure that adequate coverage is present throughout the day. The measurements are taken during the execution of the SQL testing. Table 6 contains the test results of the Wi-Fi coverage

Table 6. Wi-Fi Coverage Test Results

Time	Signal Strength (dBm)			Link Speed (Mbps)
	Maximum	Minimum	Average	
0830	38	46	41.7	400
1000	36	44	40.6	400
1130	40	46	43.1	400
1300	40	46	43.8	400
1430	44	49	46	400
1600	43	45	44.2	400

Throughout the day, the signal strength remains well within the acceptable range. According to the Keuwlsoft Wi-Fi Analyzer, anything 50 dBm or better is considered a strong signal. The worst case signal strength observed during testing is 49 dBm.

B. INTERNET SPEED TESTING

This section shows the Internet speed test results from each of the test devices. The devices were each tested in the morning and in the afternoon during high network traffic times, 10 measurements were taken for each of the devices during the morning and afternoon tests. The VPN was tested only during the afternoon because all of the testing over the VPN is accomplished during the afternoon hours. Ookla SpeedTest uses three metrics to determine Internet speeds, the ping test, upload speed, and download speed. For every test, the Sneaker Server located in San Jose was used to test the speeds. Figure 20 shows the results of the morning ping test results.

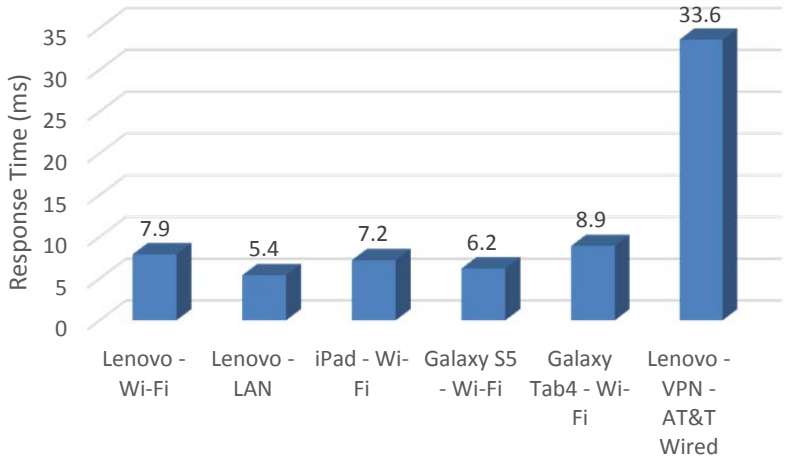

Figure 20. Morning Ookla SpeedTest Ping Results

Each of the devices tested on the Wi-Fi returned similar results, with the Lenovo connected to the hard wired LAN producing the fastest results and the Lenovo connected to the VPN through AT&T residential Internet service producing the slowest results. Figure 21 shows the results of the afternoon ping test results.

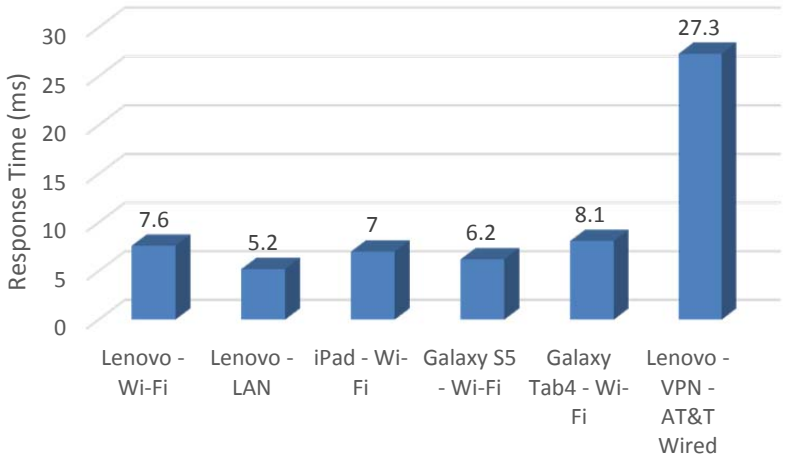

Figure 21. Afternoon Ookla SpeedTest Ping Results

Similar to the morning results, each of the Wi-Fi connected devices performed similarly with the Galaxy Tab4 producing the slowest on campus results and the Lenovo connected to the hardwired LAN again producing the fastest. The VPN connected workstation performed more than three times slower than the slowest campus Wi-Fi connected devices. Following the ping test, the upload speeds are tested. Figure 22 shows the results of the morning upload speed tests.

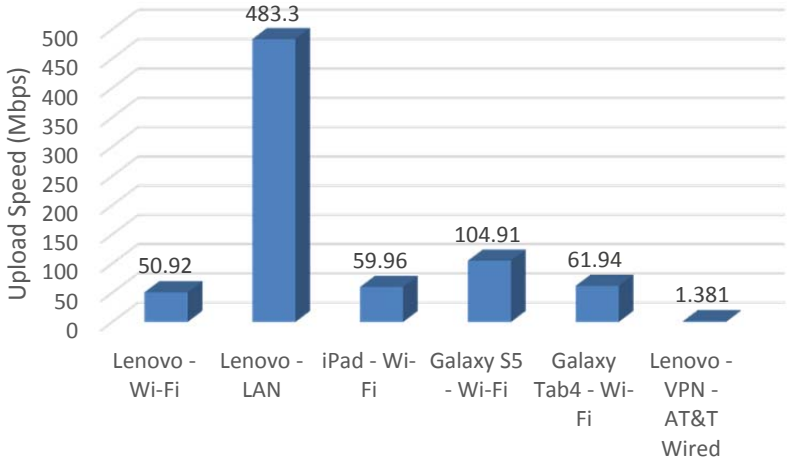

Figure 22. Morning Ookla SpeedTest Upload Results

The upload test continues the trend of the Lenovo connected to the hardwired LAN producing the fastest results, nearly five times the speed of the best Wi-Fi connected device. The slowest performing device in the morning upload test was the Lenovo connected to the VPN through the AT&T residential Internet service. Figure 23 shows the results of the afternoon upload speed tests.

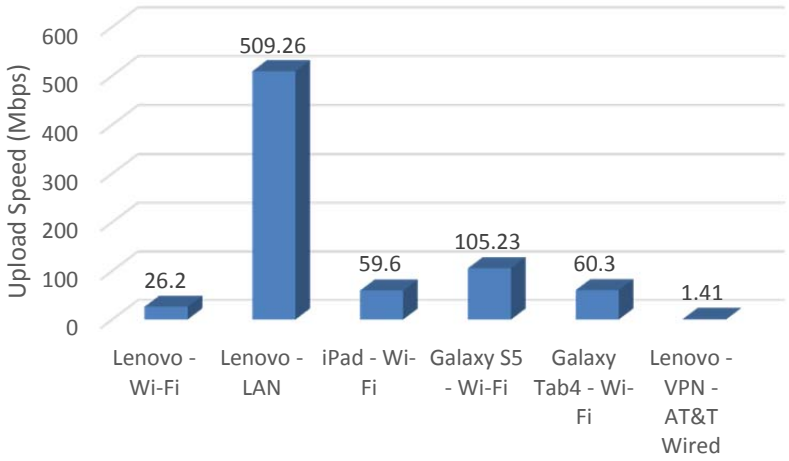

Figure 23. Afternoon Ookla SpeedTest Upload Results

Once again, the hardwired LAN connected Lenovo workstation produces the fastest results, with an even larger improvement over the next best speed when compared to the morning results. The notable data point in the upload test results is the disparity in the speed of the VPN connected workstation compared to all other devices tested. The Lenovo connected to the VPN is connected through AT&T's residential Internet service which is not nearly as fast as the campus network provided by the Naval Postgraduate School, resulting in the large disparity in the observed speeds. The third and final test performed during the Ookla SpeedTest is the download speed test, the results of the morning speed are found in Figure 24.

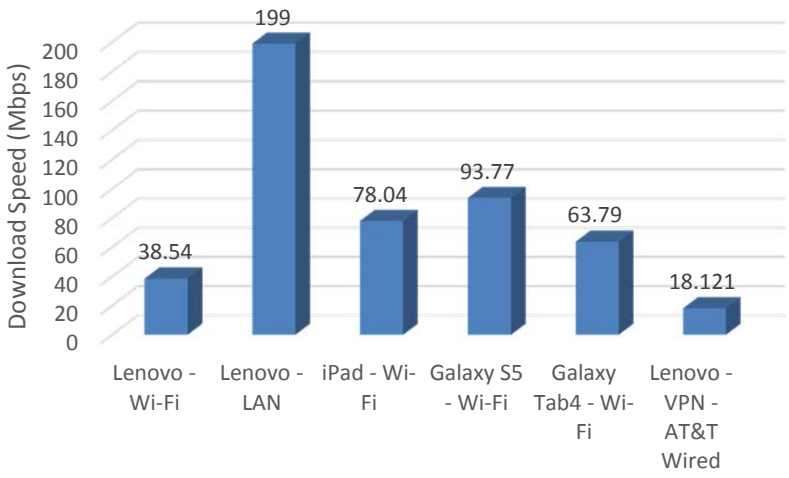

Figure 24. Morning Ookla SpeedTest Download Results

The hardwired LAN connected workstation continues to offer the best performance, while the VPN connected workstation again offers the slowest performance. The Galaxy S5 has the fastest speeds of the Wi-Fi connected devices; however, the other two mobile devices provided similar speeds. Figure 25 shows the results of the afternoon download tests.

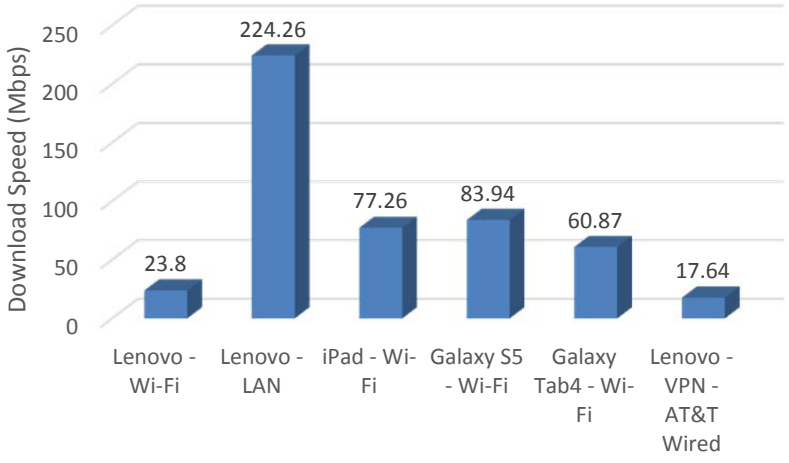

Figure 25. Afternoon Ookla SpeedTest Download Results

The hardwired connected workstation once again has the fastest tested throughput; however, the gap is not as large as with upload results. The hardwired Lenovo provided only slightly more than double the speed of the next fastest device. The Galaxy S5 offers the best Wi-Fi connected device results and the Lenovo workstation connected to the Wi-Fi is the slowest campus network connection. The VPN connected workstation is slower compared to the campus network, but by a smaller margin.

C. SQL TESTING

There are two metrics analyzed during the SQL testing, time to execute the query, and the throughput required to execute the query. Each of the five SQLs is tested with every device. The Lenovo workstation is used collect throughput data with Wireshark. The throughput is measured with direct connections to the GCSS-MC Tables database and through the VPC; both on campus through Wi-Fi and the hardwired Ethernet. The first metric that is analyzed is the SQL execution time.

1. Execution Time Analysis

The SQL execution time is determined by running it in SQL Developer and recording the time from SQL Developer to return all of the rows of the query. Each SQL is executed ten times from each device. In the case of the Lenovo workstation, the SQLs are tested using Wi-Fi and Ethernet, through both VPC and directly to the database. Figure 26 shows the average execution times for SQL1. SQL1 accesses one table in the GCSS-MC Tables database and returns 144,412 rows of data consisting of seven fields.

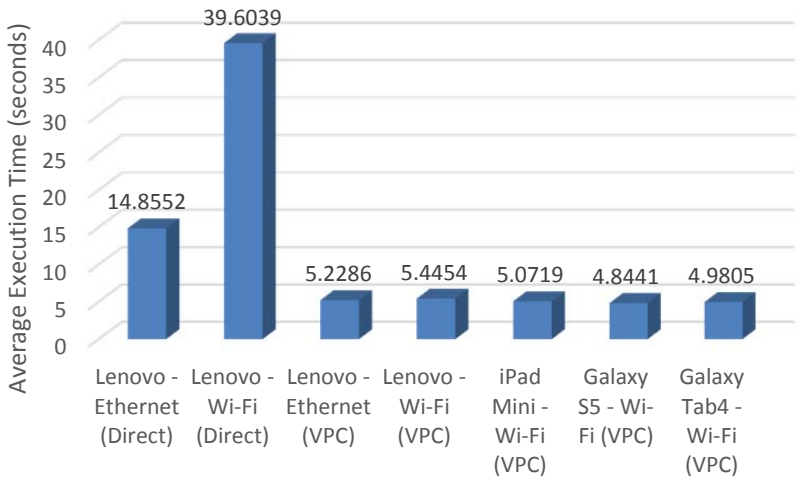

Figure 26. Average Execution Time SQL1

Figure 27 shows the average execution times for SQL2. SQL2 accesses two tables in the GCSS-MC Tables database and returns 85,606 rows consisting of seven fields.

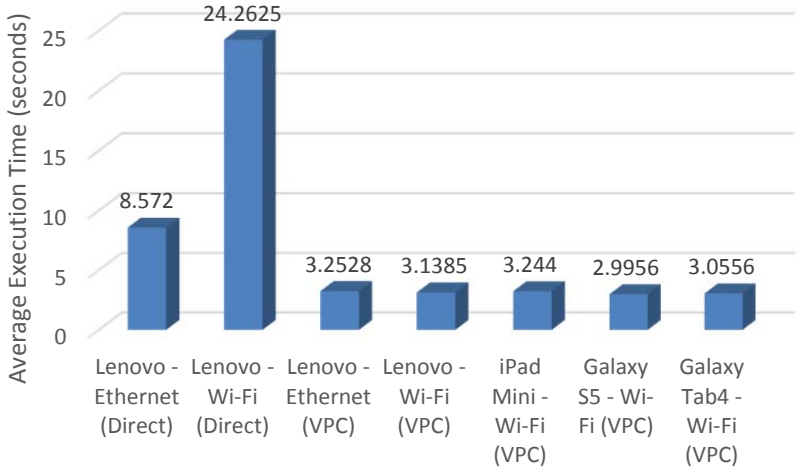

Figure 27. Average Execution Time SQL2

Figure 28 shows the average execution times for SQL3. SQL3 accesses three tables in the GCSS-MC Tables database and returns 132,983 rows consisting of five fields.

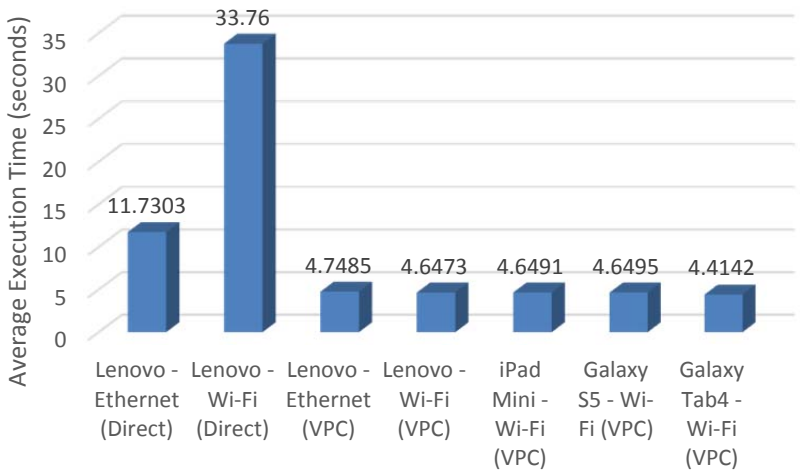

Figure 28. Average Execution Time SQL3

Figure 29 shows the average execution times for SQL4. SQL4 accesses four tables in the GCSS-MC Tables database and returns 114,339 rows consisting of five fields.

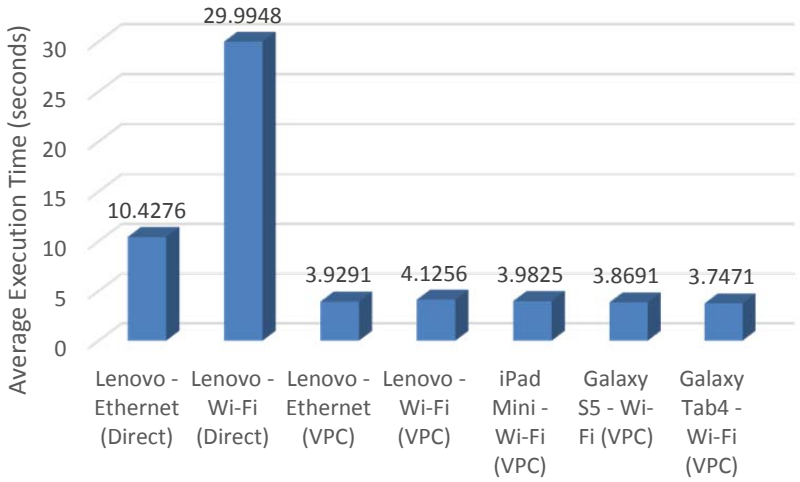

Figure 29. Average Execution Time SQL4

Figure 30 shows the average execution times for SQL5. SQL5 accesses five tables in the GCSS-MC Tables database and returns 106,162 rows consisting of nine fields.

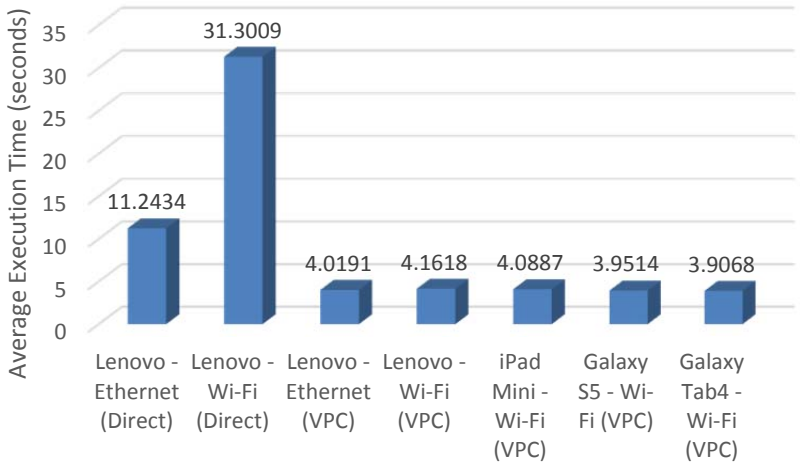

Figure 30. Average Execution Time SQL5

When examining Figures 26, 27, 28, 29 and 30, it is evident that executing the SQLs through the VPC offers a noticeable speed advantage. Anytime the VPC is used to execute the SQL, whether it is through the Lenovo workstation or a mobile device, the execution time is significantly faster. In each of the tests, the Wi-Fi connected Lenovo workstation directly accessing the database offered the slowest performance. The slow performance for the Lenovo over the Wi-Fi is a logical result, as it has the slowest upload and download speeds from the speed tests. Additionally, the type of device used to execute the SQL through the VPC does not appear to have an effect on the execution time of the SQL as the VPC returned similar results for each SQL regardless of the device accessing it. This is the logical result because the individual devices are not executing the SQL, the VPC is executing the SQL.

2. Throughput Analysis

The throughput analysis was conducted concurrently with the execution time analysis. The Lenovo workstation, running Wireshark, conducted packet captures while executing the SQLs. Both the Wi-Fi and the hard wired Ethernet connections were tested, executing all five SQLs. In Wireshark, the traffic flows were easy to isolate by applying a filter to the traffic capture such that the source or destination of the packets were the IP address of the server hosting the GCSS-MC Tables database or the IP address of the

server hosting the VPC, depending on which method was being tested. Once the filter was applied, Wireshark has tools to analyze the capture, providing statistics such as the number of packets transmitted and received, the volume of traffic transmitted and received, and the length of time of the traffic flow. The metric of interest is the total throughput when executing the SQLs.

Figure 31 shows the throughput of executing the five SQLs on the hardwired Ethernet with a direct connection to the GCSS-MC Tables database and through the VPC. The direct connection to the database uses SQL Developer on the Lenovo workstation, executes the SQL and receives the results from the database. The total throughput is significantly higher when executing a direct connection to the database than when executing the same SQL through the VPC.

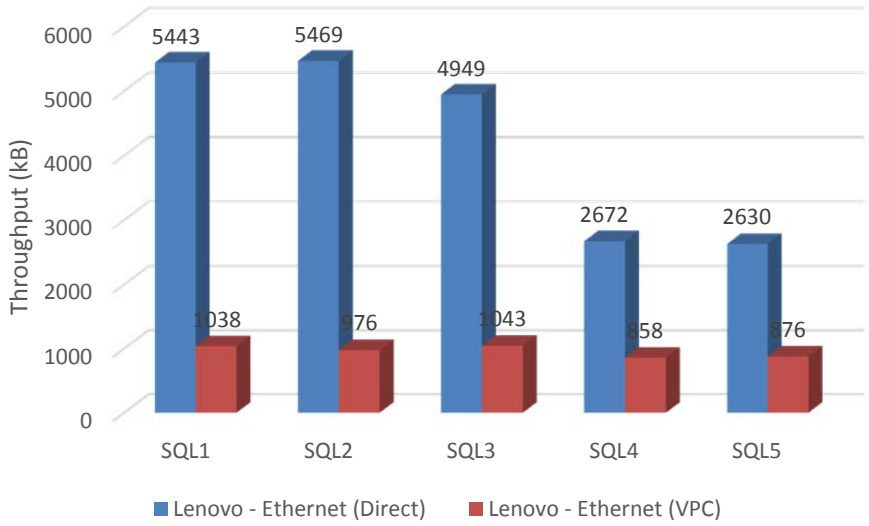

Figure 31. Total Throughput Ethernet Direct vs. VPC

Figure 32 shows the throughput of executing the five SQLs on the campus Wi-Fi with a direct connection to the GCSS-MC Tables database and through the VPC. As with Ethernet connection, there is a notable difference in the throughput with the VPC using far less throughput to execute the same SQL.

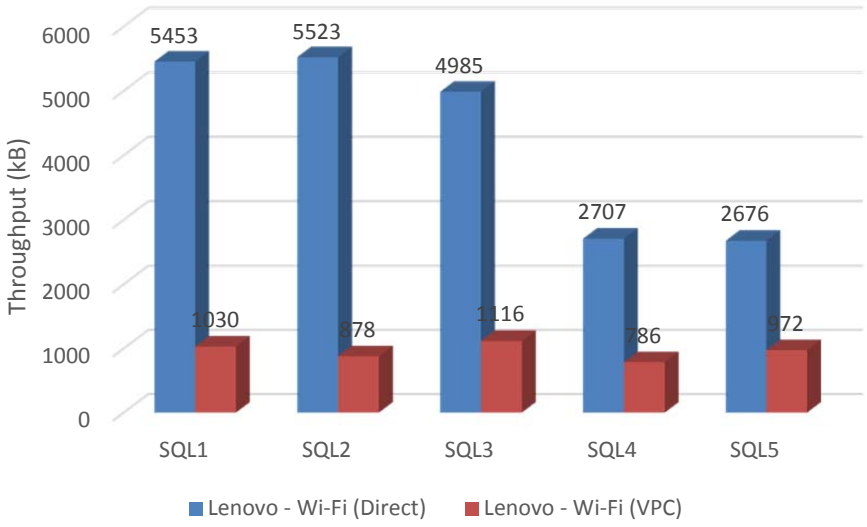

Figure 32. Throughput Wi-Fi Direct vs. VPC

Regardless of the network connection type the VPC offers a large advantage in terms of reducing required throughput to execute identical SQLs, allowing slower and less capable networks to perform on the same level as fast networks. The required throughput is reduced significantly because of the type of traffic that is transported. When directly connected to the database, the SQL is first transported to the database, the query is run on the database, then all of the data is returned to the workstation. When running the SQL through the VPC, the only thing that is communicated between the workstation and the VPC are user inputs, such as pointer and keyboard inputs, and screen images and screen updates. As the amount of data transported increases, the VPC advantage grows. Notable in both Figure 31 and Figure 32, the throughput of the direct connection to database varies significantly with each SQL, the throughput remains relatively constant when using the VPC.

D. VPN TESTING

This section shows the results of testing the five SQLs from a remote location using AT&T residential Internet service, accessing the assets on the Naval Postgraduate School network through a VPN. The Lenovo workstation used during testing, was

connected directly to the switch through a hardwired LAN. The Ookla SpeedTest results from the remote location connected to the VPN are available in Figure 20, Figure 21, Figure 22, Figure 23, Figure 24, and Figure 25. The same server from San Jose was used to conduct the SpeedTest. The same two metrics are analyzed during the VPN testing, SQL execution time and throughput required to execute the SQL. Each of the five SQLs are tested from the Lenovo workstation directly and through the VPC. Throughput data is again collected with Wireshark. The first metric analyzed is the SQL execution time.

1. Execution Time Analysis

Execution time is determined by running the SQL in SQL developer and recording the time from SQL developer of how long it took to return all of the rows from the query. Each SQL is executed ten times from the Lenovo work station directly through SQL developer to the GCSS-MC Tables database, and through the VPC. Figure 33 shows the average execution times for the five SQLs directly and the VPC.

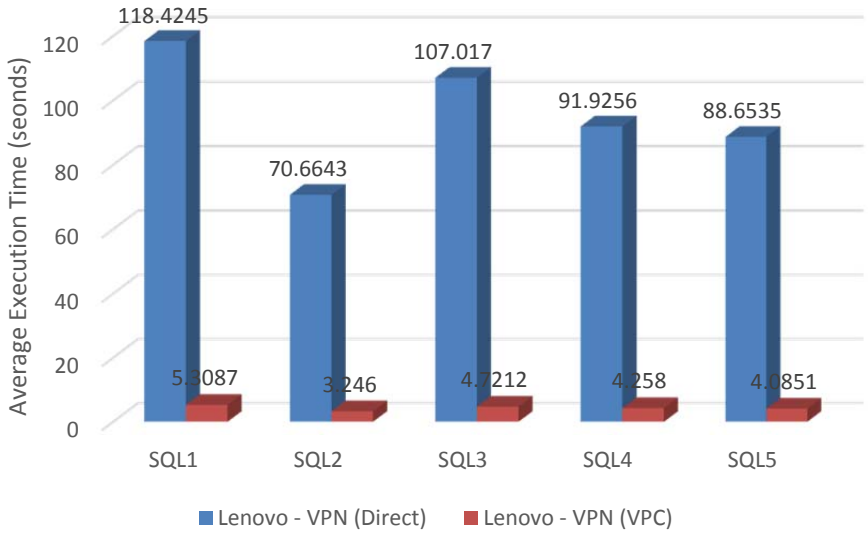

Figure 33. Average Execution Time VPN - Direct Access vs. VPC

The improvement in execution time is much larger than when testing from the campus network. This is due to the much slower network speeds when accessing the campus assets through the VPN compared to the campus network speeds. The execution

speeds of each SQL when executed through the VPC are virtually unchanged whether on the campus network or off the campus network.

2. Throughput Analysis

The throughput analysis was again conducted concurrently with the execution time analysis. The Lenovo workstation, running Wireshark, conducted packet captures while executing the SQLs. Unlike when on campus, the individual traffic flows are not isolated because all of the traffic to and from the Lenovo workstation is communicating with the VPN server. The throughput reflected in Figure 34 includes all of the overhead associated with communicating through a VPN such as the extra encryption and encapsulation that occurs.

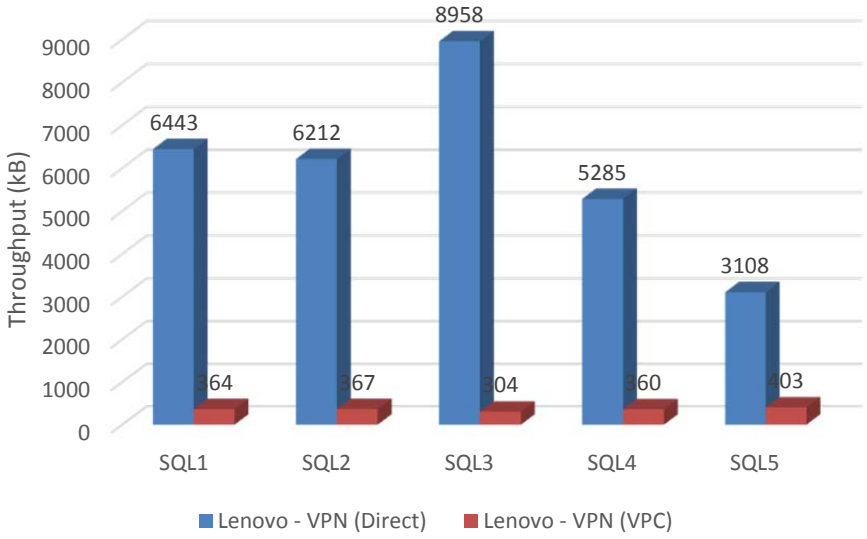

Figure 34. VPN Throughput Direct vs. VPC

As with the execution time analysis, there is an even larger improvement when executing the SQLs through the VPC over the VPN. The throughput to execute identical SQLs is dramatically decreased when accessing the VPC instead of directly accessing the GCSS-MC Tables database. When comparing the results in Figure 34 to the results in Figures 31 and 32, the throughput is decreased when accessing through the VPN. The

decrease in throughput occurs because the remote desktop protocol used by VNC Connect adapts to the network conditions and scales the throughput accordingly.

E. CHAPTER SUMMARY

Chapter IV details the experiment conducted and the results. The chapter begins with Wi-Fi coverage analysis and Internet speed testing for the networks used during experimentation. The chapter then conducts SQL testing measuring the execution time and throughput. The execution time is measured from the Lenovo workstation when connected directly to the GCSS-MC Tables database and the VPC, through both Wi-Fi and the Ethernet. Each of the mobile devices execution time is measured when accessing the VPC through the Wi-Fi. In every case, the VPC outperformed the direct manipulation of the database. Chapter IV then conducts execution time and throughput analysis when accessing the GCSS-MC Tables database and VPC through the VPN. As was the case when testing from the campus network, the VPC outperformed the direct connection and by increased margins. Chapter V provides conclusions of this experiment and recommendations for future research.

V. CONCLUSIONS AND FUTURE WORK

Chapter V provides conclusions of the evaluation of the remote and mobile access to GCSS-MC using VPCs. It also suggests topics for future work and research along the same area of research.

A. CONCLUSIONS

The purpose of this research was to provide a technologically effective method to interact with GCSS-MC in mobile settings. The capability to access GCSS-MC from a mobile device remains a valid requirement because allowing Marines to access GCSS-MC through a mobile device such as a tablet or smart phone will increase their ability to achieve mission success. This work demonstrates a proof-of-concept in Chapter IV that is secure and technologically practical. The testing provides an Operating System agnostic method to access GCSS-MC from nearly any device including tablets and smartphones.

1. Device and Operating System Agnosticism

A variety of device form factors and operating systems were tested in Chapter IV to show the use of VPCs to access GCSS-MC. As long as the VPC is configured properly to access GCSS-MC, and the end user's device is capable of accessing the VPC, end user's device has the ability to access GCSS-MC. The remote viewer used in this testing, Real VNC Viewer, is available for most laptop and mobile operating systems, including ones that were not tested during this research. This research focused on operating systems in common usage such as Windows, iOS, and Android. A variety of device types—PCs, tablets and mobile phones—were tested in this research and all were shown to have the ability to have access to the tested systems through the VPC.

2. Required Throughput Reduction

The use of a VPC drastically reduced the required throughput to accomplish identical tasks. This was shown to hold true when on the Naval Postgraduate School LAN, and when accessing the tested system through the VPN. We observed in Figure 31 on average a nearly 75% reduction in required network throughput to accomplish

identical tasks. Figure 34 shows that the advantage of using the VPC was even more evident when accessing remotely through the VPN. The required network throughput was reduced by an average of 94% to accomplish the identical tasks. When less network throughput is required, the less network resources are utilized, making the VPC a more efficient method of access, and freeing valuable network resources for use by other systems. The reduction in required network throughput is especially valuable when operating in austere deployed conditions where network resources are extremely limited.

It seems counterintuitive that required network throughput would be reduced when accessing the VPC through a VPN. As discussed in Chapter 2, a VPN encapsulates each data packet inside of an additional packet. At a minimum, the results should have shown an increase in the network throughput by the amount of the additional headers from encapsulation. The reduction in network throughput can be explained by the protocol used by the VNC Connect Viewer. RFB is an adaptive protocol which can reduce or increase the refresh rate at the client's end to match constraints imposed by network bandwidth (Richardson 2011). When accessing the VPC through the VPN, there is less available bandwidth, and the VNC Connect Viewer utilizing the RFB adapts accordingly, resulting in a reduction in the utilized network throughput. When accessing relatively static screen images as we did in this experiment, this technique works well; however, reducing the refresh rate may cause problems as the screen images become more dynamic.

3. Execution Time Reduction

The VPC displayed faster execution times than direct access to the GCSS-MC Tables database. Figures 26, 27, 28 29, and 30 show the execution times of each of the SQLs with the various devices and network types. In every case, VPC outperformed direct access. As with the required network throughput advantage, the advantage of VPC is increased when utilizing VPN. Figure 33 shows that VPC was able to execute the same SQLs in 4.5% of the time required to execute over the direct connection. Adding the extra layer of the VPN access through the AT&T residential Internet service slowed

down direct interface with the database significantly, but the user experience was largely unaffected when accessing the VPC.

B. FUTURE WORK

While constructing our proof-of-concept, areas for future research and development were identified. For the VPC method to be fully implemented for access to not just GCSS-MC, but the MCEN as a whole, there are areas that still need to be explored. The most integral future exploration is the integration of CACs and the Public Key Infrastructure (PKI) to support access control and authentication. The second area for future work is the Human Computer Interaction (HCI) aspects of using VPCs to access a complicated system such as GCSS-MC. These areas are further described in the following sections.

1. Common Access Card Integration

Currently GCSS-MC requires users to log into the system using a CAC. A user's CAC stores a copy of the user's private key, which when combined with the user's public key and the user's PIN, the user is authenticated. The VPN used in testing only requires a username and password to authenticate users. The ability to authenticate to the VPN using the user's CAC and the associated PKI needs to be investigated. Furthermore, the ability to use the credentials stored on the CAC to authenticate to GCSS-MC across the VPN needs to be verified.

2. HCI Considerations

Interactions with a system as complex as GCSS-MC may be difficult for many users. There is no mobile application, or mobile specific website associated with GCSS-MC; a user accessing GCSS-MC through a VPC would be interacting with the full version of GCSS-MC which has the potential to create HCI issues that this thesis did not address. User evaluations should occur to address issues such as which mobile device form-factor represents the most efficient method to access GCSS-MC, can a touch screen device be used to access GCSS-MC, and whether or not a small screen size makes access to GCSS-MC difficult for users. Before a VPC system is employed, HCI considerations must be evaluated to ensure that user requirements are properly considered.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Agila, Roy. 2016. “Improved Distance Learning Environment for Marine Forces Reserve.” Master’s thesis, Naval Postgraduate School. http://hdl.handle.net/10945/50459.

Arakelian, Caroline, and Chris Halstead. 2016. *Blast Extreme Display Protocol In Horizon 7*. Technical White Paper—October 2016. Palo Alto: VMware. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-horizon-7-view-blast-extreme-display-protocol.pdf.

Armbrust, Michael, Armando Fox, Rean Grifith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. 2010. “A View of Cloud Computing.” *Communications of the ACM* 53.4: 50–59.

Barreto, Albert. 2011. “Integration of Virtual Machine Technologies into Hastily Formed Networks in Support of Humanitarian Relief and Disaster Recovery Missions.” Master’s thesis, Naval Postgraduate School. http://calhoun.nps.edu/handle/10945/10736.

Bitto, Nicholas. 2014. “Adding Big Data Analytics to GCSS-MC.” Master’s thesis, Naval Postgraduate School. http://calhoun.nps.edu/handle/10945/43879.

Cisco. 2016. “Cisco AnyConnect Secure Mobility Client for Mobile Platforms Data Sheet.” Cisco. http://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/data_sheet_c78-527494.html.

Department of Defense Chief Information Officer. 2012. *Department of Defense Mobile Device Strategy Version 2.0*. Washington, DC: Office of the Department of Defense Chief Information Officer, June 8. http://www.globalsecurity.org/military/library/policy/dod/dod-mobility-strategy-v2_2012.pdf.

Farrington, Robert. 2010 “Oracle ® E-Business Suite Concepts Release 12.1” Oracle. https://docs.oracle.com/cd/E18727_01/doc.121/e12841.pdf.

Grance, Timothy and Peter Mell. 2011. *The NIST Definition of Cloud Computing*. NIST Special Publication 800–145. Gaithersburg, MD: National Institute of Standards. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Jones, Mark W. 2010 “Implementation Challenges for DOD logistics Enterprise Resource Planning IT Systems.” Master’s thesis, Naval Postgraduate School. http://calhoun.nps.edu/handle/10945/5223.

Kepes, Ben. 2016 “Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS.” Rackspace. https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/.

Keuwlsoft. 2017. Wi-Fi Analyzer. [Software]. http://keuwl.com/apps/wifianalyser/.

Kouril, Jiri, and Petra Lambertova. 2010 “Performance Analysis and Comparison of Virtualization Protocols, RDP and PCoIP.” *Latest Trends on Computers* Volume II: 782–787.

Microsoft. 2014. “Understanding the Remote Desktop Protocol (RDP)” https://support.microsoft.com/en-us/help/186607/understanding-the-remote-desktop-protocol-rdp.

Miller, Paxton L. 2016 “Mobile Support for Logistics.” Master’s thesis, Naval Postgraduate School. http://calhoun.nps.edu/handle/10945/48566.

Ookla. 2017. SpeedTest [Application]. https://www.ookla.com/.

ORACLE. 2015. SQL Developer 4.1.3.20 [Application]. http://www.oracle.com/technetwork/developer-tools/sql-developer/downloads/index.html.

———. 2016. “What Is ERP?” https://www.oracle.com/applications/erp/what-is-erp.html.

Program Executive Office for Enterprise Information Systems (PEOEIS) 2017. “Global Combat Support System-Marine Corps (GCSS-MC)” http://www.public.navy.mil/spawar/PEOEIS/Pages/GCSS-MC.aspx.

PC Magazine: “Encyclopedia.” 2017. http://www.pcmag.com/encyclopedia/.

REALVNC. 2016. “VNC Connect Security Whitepaper.” https://da7ouc4w1kep6.cloudfront.net/media/documents/vnc-connect-security-whitepaper.pdf.

Richardson, T., and Levine, J. 2011. “RFC 6143: The Remote Framebuffer Protocol” Internet Engineering Task Force. https://tools.ietf.org/html/rfc6143.

Sheneyderman, A., and Casati, A. 2003. *Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems.* Indianapolis, IN: Wiley Publishing, Inc.

Simoens, Pieter, Paul Praet, Bert Vankeirsbilck, Jeroen De Wachter, Lien Deboosere, Fiip De Turck, Bart Dhoedt, Piet Demeester. 2008 “Design and Implementation of a Hybrid Remote Display Protocol to Optimize Multimedia Experience on Thin Client Devices.” In *Proceedings of the 2008 Australasian Telecommunication Networks and Applications Conference, ATNAC 2008*: 391–396. Adelaide, Australia December 7–10.

U.S. Marine Corps Concepts and Programs. (2015). Global Combat Support System—Marine Corps. Accessed 16 February 2015. Available: https://marinecorpsconceptsandprograms.com/programs/command-and-controlsituational-awareness-c2sa/global-combat-support-system-marine-corps.

Wireshark 2.2.1(2016). Wireshark Network Protocol Analyzer [Application]. https://www.wireshark.org/download.html.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California